ANALISIS *LOSS PACKET* PADA PROSES *DOWNLOAD* DI *WIDE AREA NETWORK* MENGGUNAKAN WIRESHARK

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar
Sarjana Teknik Pada Jurusan Teknik Elektro

UIN SUSKA RIAU

Oleh :
RIO NURSAN
10655004553

JURUSAN TEKNIK ELEKTRO
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM
PEKANBARU
2013

ANALISIS LOSS PACKET PADA PROSES DOWNLOAD DI WIDE AREA NETWORK MENGGUNAKAN WIRESHARK

RIO NURSAN
NIM : 10655004553

Tanggal Sidang : 27 Juni 2013
Tanggal Wisuda : 2013

Jurusan Teknik Elektro
Fakultas Sains dan Teknologi
Universitas Islam Negeri Sultan Syarif Kasim Riau
Jl. Soebrantas No. 155 Pekanbaru

ABSTRAK

Pada saat ini perkembangan teknologi di bidang jaringan komputer sangat pesat. Hal ini dibuktikan dengan banyaknya fasilitas yang ada di internet dan meningkatnya pengguna internet. Karena banyaknya pengguna internet maka masalah pun dapat terjadi yaitu akan mengakibatkan pertukaran data melambat dan mengalami kehilangan data (*loss packet)*. Dalam penelitian tugas akhir ini analisis dilakukan dengan mengkonfigurasi router dan *sniffing* paket data saat melakukan proses *download* menggunakan program *tool network analyzer* wireshark versi 1.6.7 dengan parameter *loss packet*. Analisis dilakukan untuk meminimalisir adanya *loss packet* untuk memaksimalkan kinerja suatu jaringan. Nilai rata-rata akhir yang diperoleh berdasarkan parameter *loss packet* dari proses yang diperoleh dari percobaan download aplikasi yaitu 0,044%, dan dari streaming yaitu 22,488%.

Kata Kunci : *Loss Packet,* Router, *Sniffing, Tool Network Analyzer,* Wireshark

ANALISIS LOSS PACKET PADA PROSES DOWNLOAD DI WIDE AREA NETWORK MENGGUNAKAN WIRESHARK

RIO NURSAN
NIM : 10655004553

Date of Final Exam : June 27th , 2013
Graduation Ceremony Period : , 2013

Department of Electrical Engineering
Faculty of Science and Technology
State Islamic University of Sultan Syarif Kasim Riau
Soebrantas St. No. 155 Pekanbaru - Indonesia

ABSTRACT

At this time of technological development in the field of computer networks very rapidly. This is evidenced by the number of existing facilities on the internet and the increase of Internet users. Since the number of Internet users then problems can occur that will result in slowing down the exchange of data and experience data loss (packet loss). In this research analysis conducted by configuring routers and packet sniffing during the download process using a network analyzer tool Wireshark program version 1.6.7 with packet loss parameters. Analysis is performed to minimize the packet loss in order to maximize the performance of a network. The average value obtained by the end of the packet loss parameter of the process obtained from the trial download application that is 0.044%, and 22.488% of the stream.

Keywords: Packet Loss, Router, Sniffing, Tool Network Analyzer, Wireshark

KATA PENGANTAR

Assalamualaikum, Wr., Wb.

Alhamdullillahirobbil'alamin, puji syukur penulis ucapkan kepada Allah SWT Tuhan semesta alam yang telah melimpahkan rahmat dan hidayahnya sehingga penulis dapat menyelesaikan tugas akhir ini. Dan tak lupa pula penulis menyampaikan salawat beserta salam kepada junjungan alam yakni Nabi Muhammad SAW. Dengan limpahan kasih sayang Allah SWT penulis dapat menyelesaikan penelitian tugas akhir yang berjudul "Analisis Loss Packet pada Proses Download di Wide Area Network Menggunakan Wireshark". Tugas akhir ini disusun sebagai salah satu syarat untuk menyelesaikan studi S1 di jurusan Teknik Elektro, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sultan Syarif Kasim Riau.

Pada kesempatan ini penulis mengucapkan terima kasih kepada semua pihak yang membantu penulis baik itu berupa moral, materil, ataupun berupa pikiran sehingga terlaksananya penelitian dan penulisan laporan ini, antara lain kepada :

1. Allah SWT, atas nikmat dan karunia-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini.
2. Kedua orang tua tercinta, yang sangat penulis sayangi dan seluruh anggota keluarga atas segala do'a, nasihat dan kasih sayangnya yang tidak terhingga besarnya.
3. Ibu Dra. Hj. Yenita Morena, M.Si, selaku Dekan Fakultas Sains dan Teknologi.
4. Bapak Kunaifi, ST, PgDipEnSt, M.Sc, selaku Ketua Jurusan Teknik Elektro Fakultas Sains dan Teknologi UIN Suska Riau.
5. Bapak Abdillah, S.Si., MIT. selaku Dosen Pembimbing Tugas Akhir.
6. Seluruh Dosen Jurusan Teknik Elektro Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau yang telah banyak membimbing.
7. *My sister* (Dewi Rulyana, Ulfa Nuruliza), *my brother* (Mulya Jamil).
8. *My special one* yang selalu mendukung dalam penyelesaian Tugas Akhir ini.
9. Seluruh rekan-rekan seperjuangan Jurusan Teknik Elektro umumnya dan Angkatan 2006 khususnya.
10. Senior dan Junior Teknik Elektro UIN SUSKA RIAU.

11. Semua pihak yang telah membantu penulis dalam mengerjakan laporan ini yang tidak dapat penulis sebutkan satu persatu.

Semoga Allah SWT, Yang Maha Pengasih lagi Maha Penyayang, melimpahkan rahmat-Nya kepada Bapak/Ibu serta rekan-rekan, sebagai imbalan atas segala jasa yang telah diberikan kepada penulis.

Penulis sangat menyadari bahwa penelitian ini belum sempurna adanya, sehingga kritik dan saran dari seluruh pembaca sangat penulis harapkan demi kesempurnanya laporan penelitian ini. Demikian semoga penelitian ini dapat memberikan manfaat kepada kita semua umumnya. Khususnya bagi teman-teman yang menekuni ilmu yang sama.

Pekanbaru, 27 Juni 2013

Penulis,

Rio Nursan

DAFTAR ISI

Halaman

BAB III METODE PENELITIAN

BAB IV HASIL DAN ANALISA

BAB V KESIMPULAN DAN SARAN

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR RIWAYAT HIDUP

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan telekomunikasi dewasa ini demikian pesatnya sehingga banyak teknologi baru yang bermunculan. Adanya teknologi baru yang muncul tentu saja menawarkan lebih banyak keunggulan dan kemudahan bagi penggunanya dibandingkan teknologi pendahulunya. Sejalan dengan perkembangannya maka dibuatlah sebuah jaringan yang terdiri dari sekelompok komputer yang saling berhubungan satu sama lain dengan memanfaatkan media komunikasi, hal ini berfungsi sebagai media pertukaran data seperti melakukan pengunduhan,pengunggahan dan lain sebagainya sehingga antar komputer dapat saling berbagi dan bertukar informasi atau data.

Untuk menjembatani pertukaran informasi, transfer data antar dua jaringan yang berbeda atau di jaringan luas yang disebut dengan *Wide Area Network* (WAN) maka dibutuhkan suatu alat yang disebut router. Router berfungsi sebagai penghubung antar dua jaringan atau lebih yang dapat meneruskan data dari satu jaringan ke jaringan lainnya. Pemanfaatan penggunaan perangkat router yang tepat guna dapat dikonfigurasi berdasarkan tingkat kebutuhan tanpa mengurangi efektifitas dan kegunaannya. Hal ini merupakan salah satu alternatif tersendiri yang dapat di manfaatkan untuk mengatur atau merutekan paket data, port, protokol dan lain sebagainya.

Untuk mendapatkan performansi terbaik dari suatu jaringan maka didesainlah *Quality of Service* (QoS). Selain *browsing* jaringan lebih banyak digunakan pengguna untuk melakukan pengunduhan file atau data, semakin banyak pengguna yang melakukan pengunduhan (*download*) maka masalah pun dapat terjadi pada suatu jaringan yang akan mengakibatkan pertukaran data pada jaringan tersebut melambat dan mengalami kehilangan paket (*loss packet*) sehingga tidak sampai pada tujuan. Pengguna sangat tidak nyaman dengan adanya *loss packet* saat melakukan proses pengunduhan apa lagi jika data yang di unduh dalam jumlah yang besar, hal ini sangat merugikan bagi pengguna, selain rugi waktu pengguna juga mengalami rugi biaya. Salah satu cara untuk

mengatasi hal ini yaitu dengan menganalisis aktivitas paket data pada suatu jaringan yang disebut dengan *sniffing*. Untuk melakukan *sniffing* dibutuhkan suatu aplikasi yang dapat menangkap paket data atau informasi yang melalui jaringan yaitu wireshark. Hal ini bertujuan untuk mengetahui kesalahan yang terjadi pada suatu jaringan, dapat meminimalisir adanya *loss packet* sekaligus dapat memaksimalkan kinerja jaringan.

Dari permasalahan di atas penulis tertarik melakukan penelitian tentang *sniffing* paket data untuk menganalisis *loss packet* ketika melakukan pengunduhan pada WAN dengan judul "Analisis Loss Packet pada Proses Download di Wide Area Network menggunakan Wireshark". Penelitian ini dilakukan pada laboratorium jaringan SMK Muhammadiyah 1 Pekanbaru.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, perumusan masalah yang dibahas melalui tugas akhir ini yaitu :

1. Bagaimana menganalisis keterlambatan transfer data saat proses download dengan parameter *loss packet*.
2. Bagaimana mengatasi keterlambatan pada paket data saat proses download.

1.3 Tujuan Penelitian

Adapun tujuan yang akan dicapai pada penelitian ini adalah meminimalisir adanya *loss packet* untuk memperoleh jaringan yang lebih baik saat melakukan proses download data.

1.4 Manfaat Penelitian

Adapun manfaat pada penelitian ini yaitu :

1. Bagi Mahasiswa.
   a. Sebagai latihan menyelesaikan suatu permasalahan di bidang teknik elektro khususnya di bidang jaringan komputer.
   b. Dapat memperdalam bidang jaringan komputer dan juga sebagai penerapan teori yang didapat dibangku kuliah dengan lapangan kerja.

2. Bagi Perguruan Tinggi
   a. Untuk mengetahui sejauh mana daya serap mahasiswa dalam mengikuti perkuliahan.
   b. Untuk bahan evaluasi dalam peningkatan mutu perguruan tinggi.

1.5 Batasan Masalah

Agar tidak meluasnya pembahasan pada tugas akhir ini, penulis menentukan batasan masalah sebagai berikut :

1. Pada penelitian ini parameter yang dianalisis yaitu *loss packet* yang terjadi pada transfer data saat melakukan proses download.
2. Data yang dianalisis dalam bentuk file tangkapan (*capture file*).
3. Analisis pada penelitian ini menggunakan program wireshark versi 1.6.7 pada Linux Ubuntu 12.04.
4. Router yang digunakan yaitu Cisco Router 2600.

1.6 Sistematika Penulisan

Sistematika dari penulisan tugas akhir ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Bab ini terdiri dari latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah dan sistematika penulisan.

BAB II : TEORI DASAR

Bab ini berisikan tentang dasar teori yang digunakan pada skripsi ini meliputi router, arsitektur protokol, *Quality of Service*, teori perhitungan, *IP address* dan *wireshark network analyzer*.

BAB III : METODOLOGI PENELITIAN

Bab ini berisikan metodologi penelitian yang digunakan pada tugas akhir ini.

BAB IV : PERANCANGAN SISTEM DAN ANALISA

Bab ini menjelaskan prosedur yang digunakan dalam penelitian dan hasil yang didapat.

BAB V : KESIMPULAN DAN SARAN

Bab ini berisikan kesimpulan yang dihasilkan dari penelitian dan saran-saran untuk penelitian selanjutnya.

BAB II
TINJAUAN PUSTAKA

2.1 Teknologi Router

Router adalah perangkat yang akan melewatkan paket *Internet Protocol* (IP) dari suatu jaringan ke jaringan yang lain, menggunakan metode *addressing* dan *protocol* tertentu untuk melewatkan paket data tersebut. Router memiliki kemampuan melewatkan paket IP dari satu jaringan ke jaringan lain yang mungkin memiliki banyak jalur di antara keduanya. Router-router yang saling terhubung dalam jaringan internet turut serta dalam sebuah algoritma routing terdistribusi untuk menentukan jalur terbaik yang dilalui paket IP dari system ke system lain. Proses routing dilakukan berdasarkan lompatan demi lompatan (*hop by hop)*. IP tidak mengetahui jalur keseluruhan menuju tujuan setiap paket. IP routing hanya menyediakan IP address dari router berikutnya yang lebih dekat ke *host* tujuan dan *metric*. *Metric* yaitu sebuah nilai yang menunjukkan jarak untuk mencapai network tujuan. *Metric* tersebut menggunkan teknik berdasarkan jumlah *hop*. (Handriyanto, 2009).

Fungsi dari router adalah untuk meneruskan paket dari dua jaringan yang berbeda. Setiap router menentukan kemana suatu paket harus dialirkan berdasarkan pada tabel routing yang dimiliki pada setiap router. Tabel routing pada umumnya berisi informasi tentang alamat network tujuan, interface router yang terdekat dengan network tujuan, (Handriyanto, 2009).

Router pada dasarnya sama halnya dengan *Personal Computer* (PC). Komponen internal router sama dengan PC dan router juga membutuhkan *Operating System* (OS) untuk menjalankan aplikasinya, tetapi OS pada router disebut dengan *Internetworking Operating System* (IOS). Meskipun antara router dengan PC mirip, tetapi router dirancang untuk menentukan pemilihan jalur terbaik bagi paket data. (Muhammad Taufiq, 2010).

Gambar 2.1 Prinsip Kerja Router (Muhammad Taufiq, 2010).

Fungsi utama router adalah merutekan informasi (paket). Sebuah router memiliki kemampuan routing, artinya router secara cerdas dapat mengetahui kemana rute perjalanan paket akan dilewatkan, apakah ditujukan untuk *host* lain yang satu network ataukah berada di *network* yang berbeda (Iwan Sofana, 2010).

Jika paket-paket ditujukan untuk *host* pada network lain maka router akan meneruskannya ke network tersebut. Sebaliknya, jika paket-paket ditujukan untuk *host* yang satu network maka router akan menghalangi paket-paket keluar.

Komponen internal pada router terdiri atas *Random Access Memory* (RAM), *Non-Volatile Random Access Memory* (NVRAM), *Flash Memory*, *Read Only Memory* (ROM) dan *Interfaces.*

1. RAM disebut juga *Dynamic* RAM (DRAM) yang memiliki karakteristik dan fungsi dibawah ini:
    1. Menjaga *Address Resolution Protocol* (ARP) *ceche.*
    2. Menjaga *face switching cache.*
    3. Melakukan penjagaan paket.
    4. Memelihara antrian paket.
2. Karakteristik dan fungsi dari NVRAM :
    1. Menyediakan penyimpanan untuk *startup configuration file.*
    2. Mempertahankan isi file konfigurasi ketika router dimatikan atau *restart*.
3 Karakteristik dan fungsi dari *Flash Memory* :
    1. Memberikan software untuk memperbaharui tanpa menghapus dan mengganti *chip processor*.
    2. *Electrically Erasable Programmable Read Only Memory* (EEPROM) yaitu jenis yang secara elektronik dapat di hapus.
4. Karakteristik dan fungsi dari ROM :
    1. Menyimpan program *bootstrap* dan dasar *software* OS.
    2. Membutuhkan penggantian *chip* pada *motherboard* untuk meningkatkan mutu *software*
5. Karakteristik dan fungsi dari Interfaces :
    1. Menghubungkan router ke jaringan untuk frame yang masuk dan yang keluar.
    2. *Interface* dapat ditambah dan memisahkan *module*.

Dalam menentukan arah paket data dari satu jaringan ke jaringan yang lain tak lain disebut juga dengan routing sehingga hal ini dapat berfungsi sebagai penentu arah atau route. Routing dapat diberikan secara dinamis (*dynamic routing*) atau secara statis (*static routing*). (Muhammad Taufiq, 2010).

1. *Static Route* merupakan suatu metode routing dikonfigurasi secara manual oleh seorang administrator jaringan pada router.
2. *Dinamyc route* merupakan suatu metode routing yang melakukan penyesuain secara otomatis untuk informasi perubahan topologi dan trafik.

2.2 Access Control List (ACL)

ACL adalah daftar kondisi yang berlaku bagi perjalanan trafik ke seberang *interface* router. Daftar ini memberitahukan pada router apakah jenis paket untuk diterima atau ditolak. Penerimaan dan penolakan dapat didasarkan pada kondisi – kondisi tertentu. ACL memungkinkan pengaturan trafik dan menjamin akses dari suatu jaringan. ACL dapat diciptakan untuk semua jaringan *protocol routed*, seperti IP dan *Internetwork Packet Exchange* (IPX). ACL dapat dikonfigurasi pada router untuk mengendalikan akses ke suatu jaringan atau subnet (Iwan Sofana, 2010).

ACL harus digambarkan pada setiap *protocol*, stiap arah, atau setiap dasar *port*. Untuk mengendalikan trafik yang mengalir pada *interface*. ACL mengendalikan trafik pada satu petunjuk dalam waktu yang sama pada interface. Ada beberapa alasan penting mengapa perlu menciptakan ACL.

- Membatasi trafik jaringan dan menambah kemampuan jaringan. Dengan membatasi trafik video, sebgai contoh, ACL dapat mengurangi beban jaringan dan sebagai konsekuensi meningkatkan kemampuan jaringan.
- Menyediakan pengendalian trafik. ACL dapat membatasi pengiriman dari *update routing* jika *update* tidak diperlukan oleh karena kondisi jaringan maka banwidth akan dipertahankan.
- Menyediakan suatu tingkatan dasar keamanan untuk akses jaringan. ACL dapat memberikan satu *host* untuk mengakses bagian dari jaringan dan mencegah *host* lain mengakses area yang sama. Sebagai contoh, *host* A dijinkan untuk mengakses sumber daya jaringan dari *host* B dan dicegak untuk mengakses itu.

- menentukan jenis trafik untuk disampaikan atau dihentikan pada interface router. Mengijinkan trafik email untuk routed, tetapi menghentikan trafik telnet.
- mengujinkan administrator untuk mngendalikan apakah daerah klien dapat mengakses pada jaringan.
- melindungi *host* tertentu, mengizinkan atau menghentikan akses ke bagian dari jaringan. Mengizinkan atau menghentikan akses pada jenis file tertentu, seperti FTP atau HTTP (Muhammad Taufiq, 2010).

Ada 2 tipe access list pada cisco router yakni *Standard* ACL dan *Extended* ACL (Rahmat Rafiudin, 2006).

1. *Standard* ACL
   Standard ACL digunakan untuk filtering address sumber IP/IPX.

2. *Extended* ACL
   Extended ACL digunakan untuk filtering lebih kompleks , seperti filtering berdasarkan jenis protokol , address sumber dan tujuan , port-port sumber dan tujuan dan tipe pesan-pesan.

Tabel dibawah ini merangkum daftar tipe ACL.

Tabel 2.1 *Range* ACL

Tipe Access list	***Range* Nomor**
Standard IP Access List	1-99
Extended IP Access List	100-199

Sumber : Rahmat Rafiudin (2006)

2.3 Error Control

Error control berfungsi untuk mendeteksi dan memperbaiki error-error yang terjadi dalam transmisi frame-frame. Ada 2 tipe error yaitu frame hilang dan frame rusak. Frame hilang yaitu suatu frame gagal mencapai sisi yang lain, sedangkan frame

rusak yaitu suatu frame tiba tetapi beberapa bit-bit-nya error. Teknik-teknik umum untuk error control, sebagai berikut :

1. Deteksi error (*Error detection*) yaitu biasanya menggunakan teknik CRC (Cyclic Redundancy Check)
2. Positive acknowledgment : tujuan mengembalikan suatu positif acknowledgment untuk penerimaan yang sukses, frame bebas error.
3. Transmisi ulang setelah waktu habis : sumber mentransmisi ulang suatu frame yang belum diakui setelah suatu waktu yang tidak ditentukan.
4. Negative acknowledgment dan transmisi ulang : tujuan mengembalikan negative acknowledgment dari frame-frame dimana suatu error dideteksi.

Sumber mentransmisi ulang beberapa frame. Mekanisme ini dinyatakan sebagai *Automatic repeat Request* (ARQ).

2.4 Arsitektur Protokol

Arsitektur protokol yang digunakan pada suatu jaringan terdiri dari *Open System Interconnection* (OSI) dan *Transport Control Protocol/Internet Protocol* (TCP/IP).

2.4.1 Model Referensi OSI

OSI Layer adalah suatu model konseptual yang terdiri atas tujuh layer, yang masing-masing layer tersebut mempunyai fungsi yang berbeda. OSI dikembangkan oleh badan Internasional yaitu *International Organization for Standardization* (ISO) pada tahun 1977. Diasumsikan sebagai kamus, yaitu sebagai penerjemah berbagai macam bahasa dengan tujuan untuk memudahkan seseorang agar mengerti bahasa seseorang yang berbeda daerah maupun negaranya (Iwan Sofana, 2010).

Prinsip OSI Layer adalah menjadi penerjemah berbagai macam kebutuhan jaringan yang diproduksi berbagai macam perusahaan seperti Huawei, D-link, dan lain sebagainya. sebagai kesemua merk itu dapat tetap padu dan berjalan bersama. Walaupun terhitung tidak sukses dalam implementasi, namun penting untuk mempelajarinya karena sering kali OSI dijadikan referensi dan standar perbandingan dengan model network yang lain.

OSI terdiri atas 7 layer yaitu :

1. Layer 7 (*Application Layer*)

   Berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. Protokol yang berada dalam lapisan ini adalah HTTP, FTP, SMTP, dan *Network File System* (NFS).

2. Layer 6 (*Presentation Layer*)

   Berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protokol yang berada dalam level ini adalah perangkat *redirector software*, seperti layanan *workstation* dalam Windows NT dan juga *Virtual Network Computing* (VNC) atau *Remote Desktop Protocol* (RDP).

3. Layer 5 (*Session Layer*)

   Berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Selain itu, di level ini juga dilakukan resolusi nama.

4. Layer 4 (*Transport Layer*)

   Berfungsi untuk memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Selain itu, pada level ini juga membuat sebuah tanda bahwa paket diterima dengan sukses (*acknowledgement*), dan mentransmisikan ulang terhadp paket-paket yang hilang di tengah jalan.

5. Layer 3 (*Network Layer*)

   Berfungsi untuk mendefinisikan alamat-alamat IP, membuat header untuk paket-paket, dan kemudian melakukan routing melalui *internetworking* dengan menggunakan router dan *switch* layer-3.

6. Layer 2 (*Data Link Layer*)

   Befungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut sebagai frame. Selain itu, pada level ini terjadi koreksi kesalahan, *flow control*, pengalamatan perangkat keras seperti *Media Access Control Address* (MAC

Address), dan menetukan bagaimana perangkat-perangkat jaringan seperti *hub, bridge, repeater,* dan *switch* layer 2 beroperasi. Spesifikasi *Intstitute of Electrical and Electronics Engingeers* (IEEE) 802, membagi level ini menjadi dua level yaitu lapisan *Logical Link Control* (LLC) dan lapisan MAC.

7. Layer 1 (*Physical Layer*)

   Berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan seperti Ethernet atau Token Ring, topologi jaringan dan pengabelan. Selain itu, level ini juga mendefinisikan bagaimana *Network Interface Card* (NIC) dapat berinteraksi dengan media kabel atau radio.

2.4.2 Model Referensi TCP/IP

TCP/IP adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet (Iwan Sofana, 2010).

TCP/IP terdiri atas 4 layer yaitu :

1. *Application Layer*

   Protokol pada layer aplikasi TCP/IP menyediakan servis-servis bagi. Software-software yang berjalan pada direct. Layer aplikasi tidak menyediakan software itu sendiri tapi hanya menyediakan servis-servis yang di dimanfaatkan oleh software yang berjalan pada direct kita, misalnya Mozilla Firefox yang berjalan pada direct kita memanfaatkan direct *Hyper Text Transfer Protocol* (HTTP) untuk mengakses suatu halaman web. Beberapa direct yang beroperasi pada layer ini antara lain : HTTP, *File Transfer Protocol* (FTP), *Post Office Protocol version 3* (POP3) dan *Simple Mail Transport Protocol* (SMTP).

2. *Transport Layer*

   Transport layer terdiri dari 2 buah direct utama yaitu TCP dan *User Datagram Protocol* (UDP). *Transport layer* menyediakan servis yang akan digunakan oleh *Application Layer*, misalnya: HTTP software meminta TCP untuk menjamin sampainya data pada tujuan, jika terjadi gangguan pada saat transmisi maka HTTP

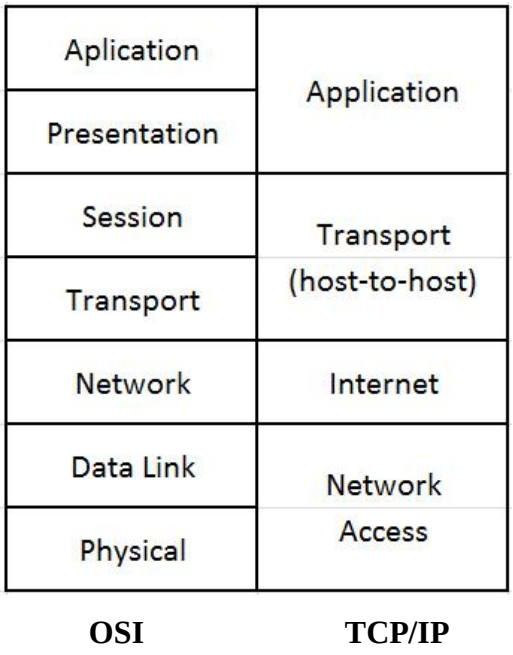
tidak akan melakukan apa-apa, tapi TCP akan mengirim ulang data yang hilang dan memastikan sampainya data pada tujuan.

3. *Internet Layer*

   Internet Layer menyediakan fungsi IP addressing, routing dan penentuan path terbaik.

4. *Network Access Layer*

   Network Access Layer mendefinisikan direct-protokol dan hardware yang digunakan untuk pengiriman data misalnya pemberian header dan trailer sehingga data dapat melewati tipe-tipe network yang berbeda. Protokol pada layer ini antara lain *Ethernet* pada jaringan *Local Area Network* (LAN) atau *Point-to-Point Protocol* (PPP) pada WAN dan *Frame Relay*.



Gambar 2.2 OSI layer dan TCP/IP layer

2.5 *Bandwidth*

Bandwidth adalah banyaknya data dalam satuan *bits per second* yang dapat ditransmisikan lewat sebuah medium jaringan dalam satu satuan waktu (Tanenbaum, 2003). *Bandwidth* terbagi atas 2, yaitu *Digital bandwidth* dan *Analog bandwidth.*

Digital bandwidth merupakan jumlah data yang dapat dikirimkan dalam jangka waktu tertentu. Satuan dari *Digital bandwidth* yaitu *bits per second* (bps) (Forouzan, 2003). *Analog bandwidth* merupakan perbedaan antara jumlah frekuensi terendah dan frekuensi tertinggi dalam sebuah rentang frekuensi yang dapat menentukan berapa banyak informasi yang dapat ditransmisikan dalam satu saat. Satuan dari *Analog bandwidth* yaitu *Hertz* (Hz) (Tanenbaum, 2003).

Bandwidth harus diperhitungkan agar dapat memenuhi kebutuhan pelanggan yang dapat digunakan menjadi parameter untuk menghitung jumlah peralatan yang di butuhkan dalam suatu jaringan. Perhitungan ini juga sangat diperlukan dalam efisiensi jaringan dan biaya serta sebagai acuan pemenuhan kebutuhan untuk pengembangan di masa mendatang. *Loss Packet* merupakan masalah yang berhubungan dengan kebutuhan bandwidth, namun lebih dipengaruhi oleh stabilitas rute yang dilewati data pada jaringan, metode antrian yang efisien, konfigurasi pada router, dan penggunaan kontrol terhadap kelebihan beban data (kongesti) pada jaringan. *Loss Packet* terjadi ketika terdapat penumpukan data pada jalur yang dilewati dan menyebabkan terjadinya overflow buffer pada router (Tanenbaum, 2003).

2.6 *Quality of Service* (QoS)

Qos adalah kemampuan suatu jaringan untuk menyediakan layanan yang baik. QoS mengacu pada kemampuan jaringan untuk menyediakan layanan yang lebih baik pada trafik jaringan tertentu melalui teknologi yang berbeda-beda. Tujuan dari QoS adalah untuk memenuhi kebutuhan layanan yang berbeda, yang menggunakan infrastruktur yang sama. Pada QoS terdapat beberapa parameter yaitu *troughtput*, *loss packet*, *delay* dan *jitter*.

2.6.1 *Troughput*

Troughput yaitu kecepatan (*rate*) transfer data efektif, yang diukur dalam bps. *troughput* merupakan jumlah total kedatangan paket yang sukses yang diamati pada *destination* selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut. *Troughput* dapat dihitung dengan rumus berikut ini :

$$Troughput = \frac{\text{Jumlah data yang dikirim}}{\text{Waktu pengiriman data}}$$

2.6.2 *Loss Packet*

Loss packet adalah banyaknya paket yang hilang selama proses transmisi dari sumber ke tujuan, *loss packet* dapat terjadi karena tabrakan data (*collision*), penurunan signal dalam media jaringan, dan kesalahan hardware pada jaringan, hal ini berpengaruh pada semua aplikasi karena *retransmisi* akan mengurangi efisiensi jaringan secara keseluruhan meskipun jumlah *bandwidth* cukup tersedia untuk aplikasi-aplikasi tersebut (Sigit Haryadi)

Dalam suatu jaringan *loss packet* akan selalu mempunyai nilai dengan satuan persen (%). Yang menjadi factor timbulnya *loss packet* adalah kepadatan *traffic* dan *bandwidth*. Semakin besar *bandwidth*, maka akan memperkecil terjadinya tabrakan data antara user yang satu dan yang lainnya. Jika terjadi *loss packet* maka protocol network yang ada pada *router* akan meminta pengirim untuk mengirim ulang paket data yang hilang tersebut. Pada saat proses pengiriman ulang data yang hilang tersebut maka akan menyebabkan meningkatnya nilai *Jitter*. Detektor dari *loss packet* berada didalam *router* yang bernama *Carrier Sense Multiplexing And Collision Detection* (CSMA-CD). Standar untuk *loss packet* adalah tidak boleh melebihi 10% dari jumlah paket data keseluruhan.

Tabel 2.2 *Loss packet*

Kategori Degradasi	Loss Packet
Sangat bagus	0 s/d 3 %
Bagus	3 s/d 15 %
Jelek	15 s/d 25 %
Sangat jelek	> 25 %

Loss Packet dapat dihitung dengan rumus :

$$\textit{Loss Packet} = \frac{\text{Paket data yang dikirim} - \text{Paket data yang diterima}}{\text{Paket data yang dikirim}} \times 100\%$$

2.6.3 *Delay*

Delay adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama. Ada beberapa jenis-jenis *delay* yaitu :

1. *Algorithmic delay, Delay* ini disebabkan oleh standar *codec* yang digunakan.
2. *Packetization delay, Delay* yang disebabkan oleh peng-akumulasian bit *voice sample* ke *frame*.
3. *Serialization delay, Delay* ini terjadi karena adanya waktu yang dibutuhkan untuk pentransmisian paket IP dari pengirim.
4. *Propagation delay, Delay* ini terjadi karena perambatan atau perjalanan.

Tabel 2.3 *Delay*

Kategori Latensi	Besar *Delay*
Sangat bagus	< 150 ms
Bagus	150 s/d 300 ms
Jelek	300 s/d 450 ms
Sangat jelek	> 450 ms

Delay dapat dihitung dengan rumus berikut ini :

$$Delay = \frac{\text{Panjang Paket (L, } \textit{packet length} \text{ (bit/s))}}{\textit{link bandwith} \text{ (R, } \textit{link bandwith} \text{ (bit/s))}}$$

2.6.4 *Jitter*

Jitter yaitu waktu yang dibutuhkan untuk sebuah paket untuk mencapai tujuan. hal ini diakibatkan oleh variasi panjang antrian dalam waktu pengolahan data, dan juga dalam waktu penghimpunan ulang paket di akhir perjalanan *jitter*. *Jitter* disebabkan oleh *Delay* antrian pada *router* dan *switch*.

Tabel 2.4 *Jitter*

Kategori Degradasi	Loss Packet
Sangat bagus	0
Bagus	0 s/d 75 ms
Jelek	75 s/d 125 ms
Sangat jelek	125 s/d 225 ms

Jitter dapat dihitung dengan rumus dibawah ini :

$$Jitter = \frac{\text{Total variasi } delay}{\text{Total paket yang diterima - 1}}$$

Total variasi *delay* diperoleh dari penjumlahan :

(*delay* 2 – *delay* 1) + (*delay* 3 – *delay* 2) + ... + (*delay* n – *delay* y (n-1))

2.7 IP *Address*

IP *address* adalah alamat identifikasi komputer yang berada didalam jaringan. Dengan adanya IP *address* maka data yang dikirimkan oleh komputer pengirim dapat dikirimkan lewat protokol TCP/IP hingga sampai ke komputer yang dituju.

IP *address* digunakan untuk menunjukkan lokasi dari perangkat dalam jaringan. IP *address* terdiri dari 32 *bit* bilangn biner yang terbagi atas empat bagian. Bagian ini dekenal sebagai *octet* atau *byte*. Masing-masing bagian terdiri atas satu *byte* (delapan *bit*) dan dapat dikonversi menjadi bilangan desimal (Iwan Sofana, 2010).

IP *address* dibedakan menjadi 3 kelas menurut ukuran jaringan secara umum.

1. Kelas A

   Kelas A menggunakan *octet* pertama untuk mendidikasikan alamat *network*. Tiga *octet* lainnya digunakan untuk mengindikasikan alamat *host*. Hal ini membuat kelas A dapat mendukung jaringan yang sangat besar dengan lebih dari 16 juta alamat *host*. Jangkauan alamat kelas A adalah 1 sampai 127 ditandai dengan *bit* pertama dari *octet* pertama harus bernilai 0 sedangkan yang lainnya adalah bebas (0xxxxxx).

2. Kelas B

   Kelas B menggunakan *octet* pertama dan kedua untuk mengindikasikan alamat *network.* Dua *octet* terakhir digunakakn untuk mengindikasikan alamat *host*. Hal ini membuat kelas B dapat mendukung jaringan dari yang sedang sampai pada jaringan yang besar dengan lebih 65000 alamat *host.* Jangkauan alamat kelas B adalah 128 sampai 191, ditandai dengan *bit* pertama dan *bit* kedua dari *octet* pertama harus bernilai 1 dan 0 sedangkan yang lainnya adalah bebas (10xxxxxx).

3. Kelas C

   Kelas C menggunakan *octet* pertama, kedua dan ketiga untuk mengindikasikan lamat *network*. *Octet* terakhir digunakan untuk mengindikasikan alamat *host.* Hal ini membuat kelas C dapat mendukung jaringan yang kecil dengan kapasitas alamat *host* sebanyak 254. Jangkauan alamat kelas C adalah 192 sampai 233 ditandai dengan *bit* pertama, kedua dan ketiga dari *octet* pertama harus bernilai 1, 1, dan 0, sedangkan yang lainnya bebas (110xxxxx).

Tabel 2.5 kelas IP *Address*

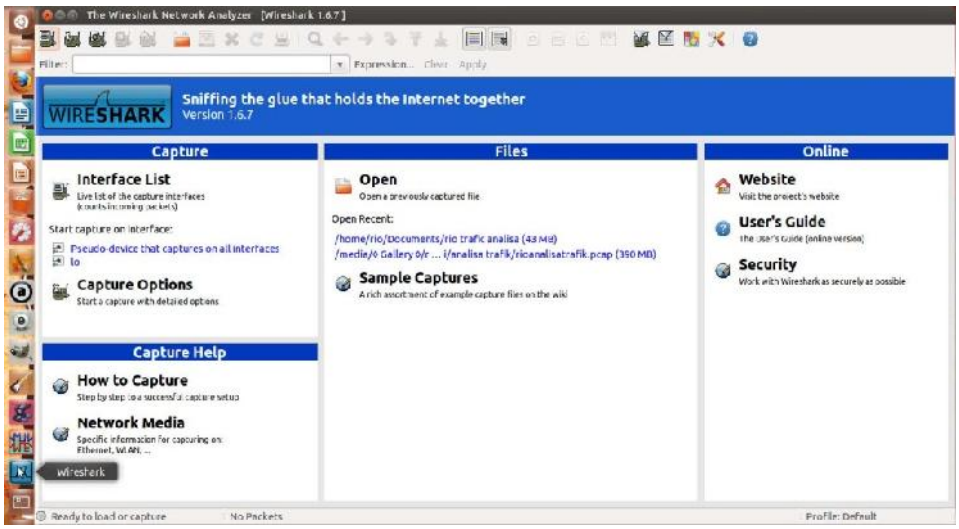
Address Class	1st octet range (decimal)	Network (N), Host (H) parts of address	Default subnet mask (decimal and binary)	IP address
A	1 – 127	N.H.H.H	255.0.0.0	10.0.0.0 – 10.255.255.255
B	128 – 191	N.N.H.H	255.255.0.0	172.16.0.0-172.31.255.255
C	192 - 233	N.N.N.H	255.255.255.0	192.168.0.0 – 192.168.255.255

2.8 *Wireshark Network Analyzer*

Wireshark merupakan salah satu aplikasi open source untuk mengetahui lalu lintas komunikasi data dalam jaringan dengan cara memantau melalui protokol dan port-port yang digunakan. Wireshark adalah salah satu dari sekian banyak tool *network analyzer* yang banyak digunakan oleh *network administrator* untuk menganalisa kinerja

jaringannya. Wireshark banyak disukai karena interfacenya yang menggunakan *Graphical User Interface* (GUI) atau tampilan grafis (Agus kurniawan, 2012).

Wireshark mampu menangkap paket-paket data atau informasi yang saling berinteraksi dalam jaringan internet. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Untuk menggunakan tool ini cukup memasukkan perintah untuk mendapatkan informasi yang ingin diperoleh dari suatu jaringan.



Gambar 2.5 Wireshark

2.9 Paket data *Sniffer, Packet Capture* dan *Packet Analyzer*

Tujuan penggunaan perangkat lunak ini adalah melihat aktivitas lalu lintas jaringan komputer, dengan melihat semua paket-paket data dari setiap protocol maka dapat terlihat segala aktivitas lalu lintas komunikasi data yang selama ini terbungkus dengan rapi. Disini dapat terlihat setiap paket data, baik yang memang merupakan sebuah serangan atau sebuah pemetaan bahkan pengenalan identitas dari perangkat keras yang akan dituju, sehingga dengan menganalisa setiap paket data tersebut dapat diambil pembelajaran mengenai keamanan data yang terdapat infrastruktur jaringan (Agus kurniawan, 2012).

1. *Packet Sniffer*

Packet sniffer berfungsi untuk menangkap pesan, data dan informasi yang sedang dikirim atau diterima oleh computer. Paket sniffer juga akan menyimpan atau menampilkan isi protocol yang berbeda pada bagian Capture Message. Packet sniffer bersifat pasif. Packet sniffer mengamati pesan yang sedang dikirim dan diterima oleh aplikasi dan protocol yang berjalan di computer.

2. *Packet Capture*

   Packet Capture menerima salinan dari setiap frame link-layer yang dikirim atau diterima oleh computer. Pesan ditukar oleh layer protocol yang lebih tinggi seperti HTTP, FTP, TCP, *User Data Protocol* (UDP), *Domain Name System* (DNS) atau IP yang semuanya itu kemudian dienkapsulasi pada frame link-layer yang ditransmisikan oleh media fisik, misalnya kabel eternet.

3. *Packet Analyzer*

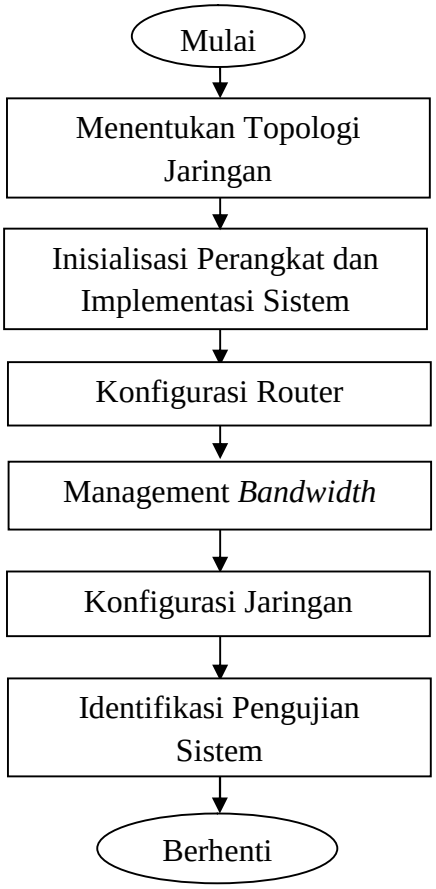
   Packet Analyzer berfungsi untuk memahami struktur data yang dikirim oleh protokol.

Dari aplikasi wireshark terlihat berbagai macam *protocol* dengan berbagai penanganan baik oleh *server* sampai hasil penanganan yang diterima oleh *client*. Dengan informasi capture yang masih mentah dan penuh dengan informasi yang perlu di saring (*filter*), maka dengan menggunakan fungsi-fungsi yang terdapat pada wireshark dapat menganalisa hasil capture tersebut.

BAB III
METODE PENELITIAN

3.1 Tahapan Penelitian

Metode penelitian merupakan dasar penyusungan langkah-langkah penelitian. Adapun tahapan yang akan dilakukan dalam melaksanakan penelitian ini yaitu menentukan topologi jaringan, melakukan mengkonfigurasi router dan perangkat PC serta instalasi perangkat lunak (*software*).



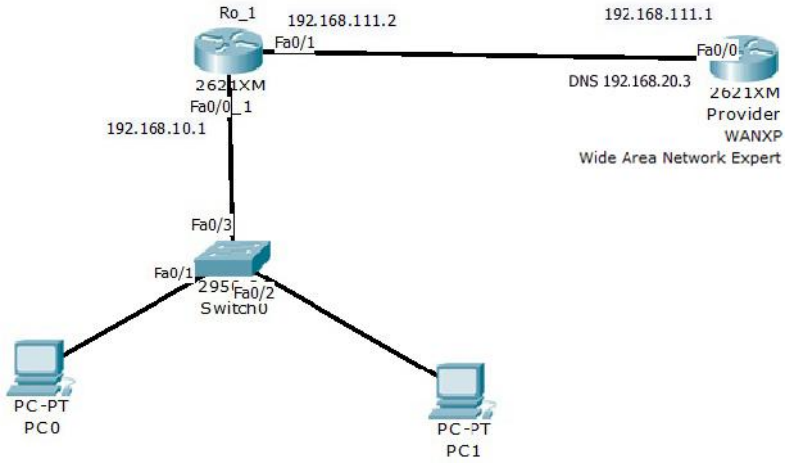
Gamabar 3.1 Flowchart Penelitian

Menentukan topologi jaringan sangat penting sebelum melakukan konfigurasi dalam suatu jaringan. Karena topologi merupakan gambaran bagaimana suatu perangkat jaringan dapat berkomunikasi. Pada konfigurasi router dan perangkat PC terdapat beberapa tahapan kerja. Tahapan kerja yang dimaksud yaitu menghubungkan perangkat

jaringan dan melakukan konfigurasi pada perangkat jaringan. Pada tahapan instalasi perangkat lunak penulis menggunakan wireshark untuk mendapatkan hasil yang akan dianalisis nantinya.

3.2 Topologi Jaringan

Topologi jaringan adalah hal yang menjelaskan hubungan geometris antara unsur-unsur dasar penyusun jaringan, yaitu node, link, dan station.



Gambar 3.2 Topologi jaringan penelitian

3.3 Inisialisasi Peralatan dan Implementasi Sistem

Sebelum melakukan konfigurasi jaringan, pada dasarnya setiap jaringan yang ingin dibuat memerlukan prasarana penunjang untuk mengimplementasikan konfigurasi pada jaringan tersebut. Adapun perangkat yang dibutuhkan yaitu *Hardware* yaitu berfungsi sebagai tempat mengolah data dan untuk melakukan konfigurasi alat yang akan di gunakan, kemudian *Software* yaitu perangkat lunak yang dibutuhkan untuk menganalisa data jaringan yang telah terhubung.

1. Perangkat Router dengan spesifikasi :

Router Type	:	Cisco Router 2600
Fast thernet (10/100)	:	2
Network Module Slot	:	1
WAN Interface Card Slots	:	2
Advanced Integration Module Slots	:	1

Gambar 3.3 Cisco router 2600

2. Perangkat PC yang digunakan untuk konfigurasi router dengan spesifikasi :

Gambar 3.4 Perangkat konfigurasi Router

PC Type	:	*Hawlett-Packard* (HP) PC
Processor	:	AMD 2.4 GHz
RAM	:	2 Gb
Harddisk	:	250 Gb
Sistem operasi	:	Windows XP

3. Perangkat PC digunakan untuk menganalisa paket data yang melalui suatu jaringan dengan spesifikasi sebagai berikut :

PC Type	:	Acer Aspire 4736
Processor	:	Intel Core 2 Duo 2.20 GHz
RAM	:	2 Gb
Harddisk	:	320 Gb
Sistem operasi	:	Linux Ubuntu 12.04

Gambar 3.5 Perangkat Analisa Data

4. Kabel USB-RS232.

Gambar 3.6 Kabel USB-RS232

Spesifikasi kabel : USB-RS232 serial interface with integrated 2 m USB-A cable, D-SUB 9-pin male connector

Jenis Kabel yang digunakan untuk melakukan konfigurasi router yaitu kabel USB-RS232 yang berfungsi sebagai penghubung kabel *console* router ke usb PC.

5. Lokasi Penelitian dan Perangkat Lunak :

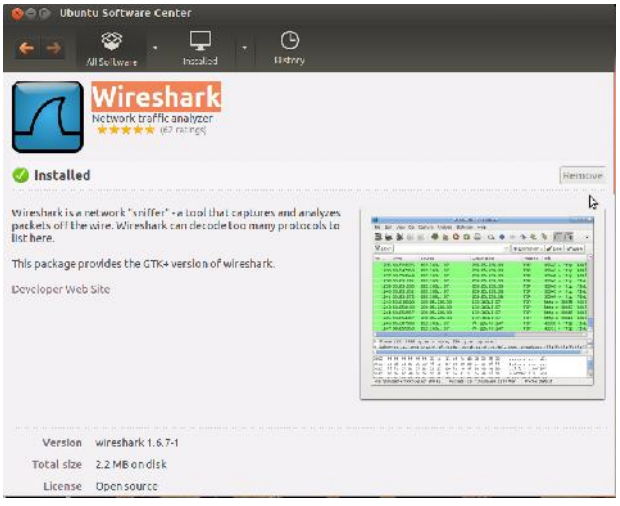
Lokasi Penelitian	: SMK MUHAMMADIYAH 1 PEKANBARU
Provider	: WAN Expert, up to 2 MBps (Hegal Optilisnur)
Sistem Operasi	: Windows XP untuk konfigurasi router , Linux Ubuntu 12.04 untuk menganalisis
Tools	: Wireshark versi 1.6.7 for linux
Browser	: Mozilla Firefox versi 20

6. Perangkat switch yang digunakan yaitu D-Link switch

D-Link Switch Type	: D-Link DES-1008D
Port	: 8 port 10/100Mbps Auto-sensing
Media Interface	: RJ-45

Gambar 3.7 D-Link Switch

7. Instalasi Wireshark pada Linux

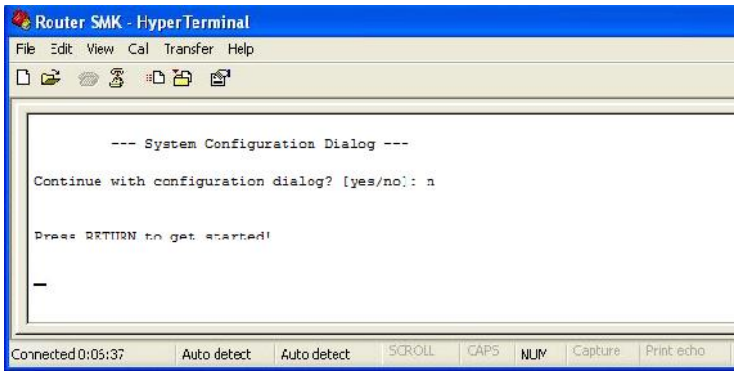


Gambar 3.8 Instalasi Wireshark

Pada gambar 3.8 adalah proses instalasi wireshark yang berfungsi untuk menganalisis trafik data yang melalui sebuah jaringan, aplikasi wirehark di instal dengan memanfaatkan *Ubuntu Software Center* pada sistem operasi Ubuntu 12.04. Instalasi aplikasi wireshark ini terhubung dengan jaringan internet karena proses instalasi memerlukan pengunduhan aplikasi wireshark.

3.4 Konfigurasi Router

Konfigurasi router dilakukan menggunakan HP PC dan aplikasi yang digunakan untuk melakukan konfigurasi pada router yaitu *Hyper Terminal* yang telah tersedia pada sistem operasi *Windows XP*. Untuk menggunakan *Hyper Terminal* terlebih dahulu klik *Start* kemudian *All Programs* lalu pilih *Accessories*, masuk ke *Communications* dan pilih *Hyperterminal*. Kemudian menuliskan nama dan menentukan *serial port* yang dihubungkan dengan kabel *console*.



Gambar 3.9 *Hyperterminal*

Gambar 3.9 adalah tampilan *hyperterminal* saat mulai melakukan konfigurasi terhadap router yang terhubung melalui kabel USB-RS232. Pada konfigurasi router terdapat beberapa tahapan kerja, antara lain :

3.4.1 Menentukan *Hostname*

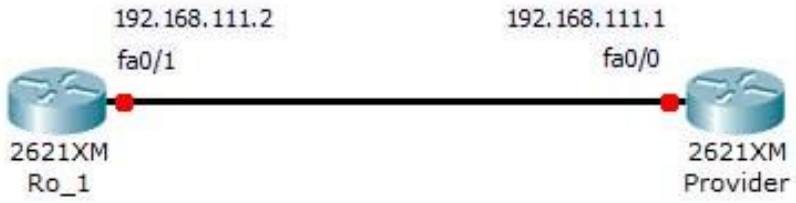
Dalam mengkonfigurasi router hal pertama yang dilakukan yaitu memberi nama pada router. Pembarian nama pada router dilakukan agar setiap komputer dapat berkomunikasi antara satu dengan lainnya. Router pertama diberi nama Ro_1. Perintah

Command Line Interface (CLI) yang digunakan untuk memberi nama pada Ro_1 adalah sebagai berikut :

```
Router>enable
Router#conf t
Router(config)#hostname Ro_1
Ro_1 (config)#
```

3.4.2 *Setting* IP *Address* Router

Melakukan konfigurasi IP *address* router dengan IP *address interface* FastEthernet0/1 Ro_1 adalah 192.168.111.2 dan FastEthernet0/0 Ro_1 adalah 192.168.10.1. Kedua router akan dihubungkan dengan masing-masing IP *address interface* adalah 192.168.111.1 dan 192.168.111.2 dengan netmask standar.



Gambar 3.10 Konfigurasi IP *Address*

Perintah CLI yang digunakan untuk melakukan konfigurasi IP *address* adalah sebagai berikut :

```
Ro_1(config)#int fa0/0
Ro_1(config-if)#IP address 192.168.10.1 255.255.255.0
Ro_1(config-if)#no shut
Ro_1(config-if)#int fa0/1
Ro_1(config-if)#IP address 192.168.111.2 255.255.255.0
Ro_1(config-if)#no shut
Ro_1(config-if)#exit
```

3.4.3 Menentukan IP *Route*

Routing protocol akan menentukan jalur yang dilalui oleh sebuah paket melalui sebuah *internetwork*. Jalur pertama yang harus dilewati paket data untuk dapat masuk ke network yang lain. Pada Ro_1 jika ingin mencapai network 192.168.111.1 harus melalui IP address 192.168.111.2. Perintah CLI IP *route* pada router sebagai berikut:

```
Ro_1(config)#IP route 0.0.0.0 0.0.0.0 192.168.111.1
```

3.4.4 *Dynamic Host Configuration Protocol* (DHCP)

DHCP digunakan untuk memberikan nomor IP kepada komputer yang memintanya. Komputer yang memberikan nomor IP disebut sebagai DHCP server, sedangkan komputer yang meminta nomor IP disebut sebagai DHCP Client. Dengan demikian administrator tidak perlu lagi harus memberikan nomor IP secara manual pada saat konfigurasi TCP/IP, tapi cukup dengan memberikan referensi kepada DHCP Server.

Pada saat kedua DHCP client dihidupkan , maka komputer tersebut melakukan request ke DHCP-Server untuk mendapatkan nomor IP. DHCP menjawab dengan memberikan nomor IP yang ada di database DHCP. DHCP Server setelah memberikan nomor IP, maka server meminjamkan (lease) nomor IP yang ada ke DHCP-Client dan mencoret nomor IP tersebut dari daftar pool. Nomor IP diberikan bersama dengan subnet mask dan default gateway. Jika tidak ada lagi nomor IP yang dapat diberikan, maka client tidak dapat menginisialisasi TCP/IP, dengan sendirinya tidak dapat tersambung pada jaringan tersebut.

```
Ro_1(config)#IP dhcp pool LAN_KELAS
Ro_1(dhcp-config)#network 192.168.10.0 255.255.255.0
Ro_1(dhcp-config)#default-router 192.168.10.1
Ro_1(dhcp-config)#dns-server 192.168.20.3
Ro_1(dhcp-config)#exit
Ro_1(dhcp-config)#IP dhcp excluded-address 192.168.10.1
```

3.4.5 Mengaplikasikan ACL

ACL berfungsi untuk mengatur trafik dan menjamin akses dari suatu jaringan. Perintah ACL yang digunakan untuk mengizinkan trafik yang berasal dari IP address 192.168.10.1 yaitu:

```
Ro_1(config)#access-list 1 permit 192.168.10.1
```

3.4.6 Konfigurasi *Network Address Translation*

Network Address Translation (NAT) adalah suatu cara untuk menghubungkan jaringan private ke internet menggunakan satu IP public.

1. FastEthernet0 (fa0/0) dengan IP 192.168.10.1. Interface ini terhubung ke jaringan yang akan di NAT
2. FastEthernet1 (fa0/1) dengan IP 192.168.111.2. Interface ini terhubung ke internet.

Perintah CLI yang digunakan untuk konfigurasi NAT pada router :

```
Ro_1(config)#ip nat inside source list 1 interface fa0/1
overload
Ro_1(config)#int fa0/1
Ro_1(config-if)#ip nat outside
Ro_1(config-if)#int fa0/0
Ro_1(config-if)#ip nat inside
Ro_1(config-if)#exit
```

3.5 Managemen *Bandwidth*

Management *bandwidth* yaitu suatu cara yang digunakan untuk memanagemen dan memaksimalkan suatu jaringan. Managemen *bandwidth* bertujuan untuk mengatur *bandwidth* jaringan dan memberikan limit sesuai dengan kebutuhan. Adapun langkah yang di lakukan untuk memanagemen *bandwidth* pada router yaitu :

3.5.1 Menentukan *Class-Map*

Class-map dibuat untuk mengklasifikasikan atau mengatur lalu-lintas data (*traffic*) menjadi beberapa kelompok. Pengaturan ini berguna agar suatu jaringan memiliki kemampuan menyediakan jaminan dan kehandalan layanan. Untuk membuat c*lass-map* printah yang digunakan yaitu :

```
Ro_1>enable
Ro_1#conf t
Ro_1(config)#class-map LAN_KELAS
Ro_1(config-cmap)#match protocol LAN_KELAS
```

Match protokol digunakan sebagai penghubung antar protokol sehingga dapat diberikan prioritas.

3.5.2 Menentukan Aturan *Traffic*

Aturan *traffic* digunakan untuk menentukan besar *bandwidth* yang akan diberikan pada kelompok yang telah dibuat pada *class-map*. Adapun perintah yang digunakan yaitu :

```
Ro_1(config-cmap)#bandwidth percent 50
Ro_1(config-cmap)#exit
```

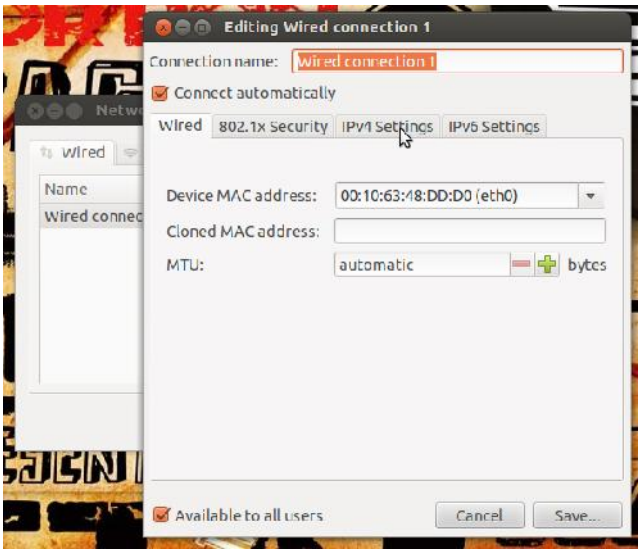
Perintah `bandwidth percent 50` diatas menyebutkan jumlai *bandwidth* (kbps) yang digunakan. Nilai 50% yang tersedia dari *bandwidth* disediakan untuk class-map yang memungkinkan protocol untuk menggunakan 50% dari link *bandwidth* pada ke-2 *client*. Hal ini dilakukan agar masing-masing *client* tidak saling memperebutkan *bandwidth* ketika melakukan proses download yang nantinya mengakibatkan terjadinya *loss packet*.

3.6 Konfigurasi Jaringan

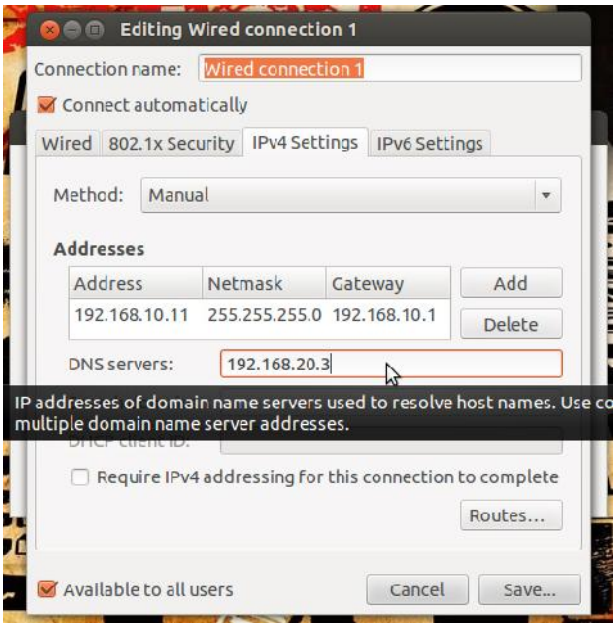
Sebelum wireshark di gunakan sebagai aplikasi untuk menganalisa paket data maka terlebihdahulu melakukan *setting* IP *address* pada Acer PC, agar wireshark dapat membaca paket data yang melalui jaringan.

3.6.1 Setting IP *address* PC

Pada gambar 3.11 menjelaskan langkah dalam pengaturan IP *address* dengan cara masuk ke *network conection* kemudian pilih *wired conection 1* pada tab wired, klik *edit* dan masuk ke tab IP*v4 Settings*, pada *Method* ganti *Automatic* (DHCP) dengan manual, dan masukkan IP Address sesuai dengan IP address yang telah di konfigurasi pada router sebelumnya.



Gambar 3.11 *Setting* IP *Address*



Gambar 3.12 IPv4 *Settings* IP *Address*

Gambar 3.12 menjelaskan cara menambahkan IP *Address* manual, klik *add* kemudian mengisi *address, Netmask, Gateway dan DNS servers.* Pada penelitian ini penulis menggunakan IP *address* kelas C, yaitu IP *address* 192.168.10.11 maka *netmask* nya otomatis 255.255.255.0, *Gateway* dan *DNS server* di setting berdasarkan konfigurasi router yaitu 192.168.10.1 untuk *Gateway* dan 192.168.20.3 untuk *DNS server.*

Setelah melakukan setingan IP *address* pada PC maka wireshark sudah bisa di gunakan untuk menganalisa paket data yang melalui jaringan.

3.7 Pengujian Sistem

Setelah melakukan konfigurasi pada perangkat dan melakukan instalasi wireshark maka dilakukan pengujian sistem. Pengujian sistem ini bertujuan untuk menemukan kesalahan atau kekurangan pada perangkat yang diuji, apakah sudah berjalan sesuai tujuan atau masih terdapat kesalahan.

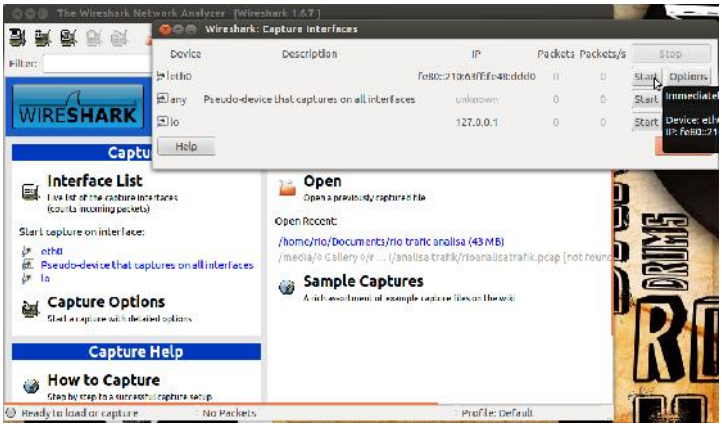
3.7.1 Melakukan *Sniffing*

Sniffing dilakukan untuk melihat paket data yang berisi informasi mengenai apa saja yang sedang berjalan pada suatu jaringan, termasuk mengidentifikasi paket data yang hilang.

Setelah melakukan instalasi wireshark pada Ubuntu 12.04, pilihan *interfaces* pada menu *capture* belum dapat digunakan, untuk itu perlu menambahkan perintah berikut ini pada terminal Ubuntu 12.04 :

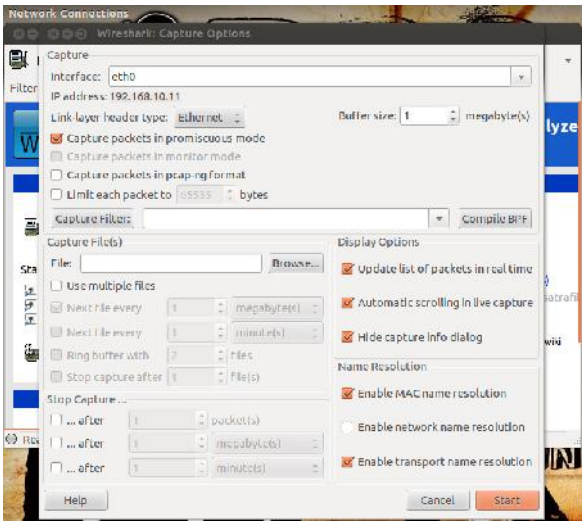
```
sudo addgroup -quiet -system wireshark
sudo chown root:wireshark /usr/bin/dumpcap
sudo setcap cap_net_raw,cap_net_admin=eip /usr/bin/dumpcap
sudo usermod -a -G wireshark Rio_Nursan
```

Gambar 3.13 Berikut ini adalah tampilan saat memilih menu *capture*, kemudian pilih *interfaces*. Pada kotak dialog terdapat daftar antarmuka jaringan yang dimiliki. Pada antarmuka ini user dapat melakukan konfigurasi dengan mengklik tombol *options* pada kotak dialog *wireshark capture interfaces*.

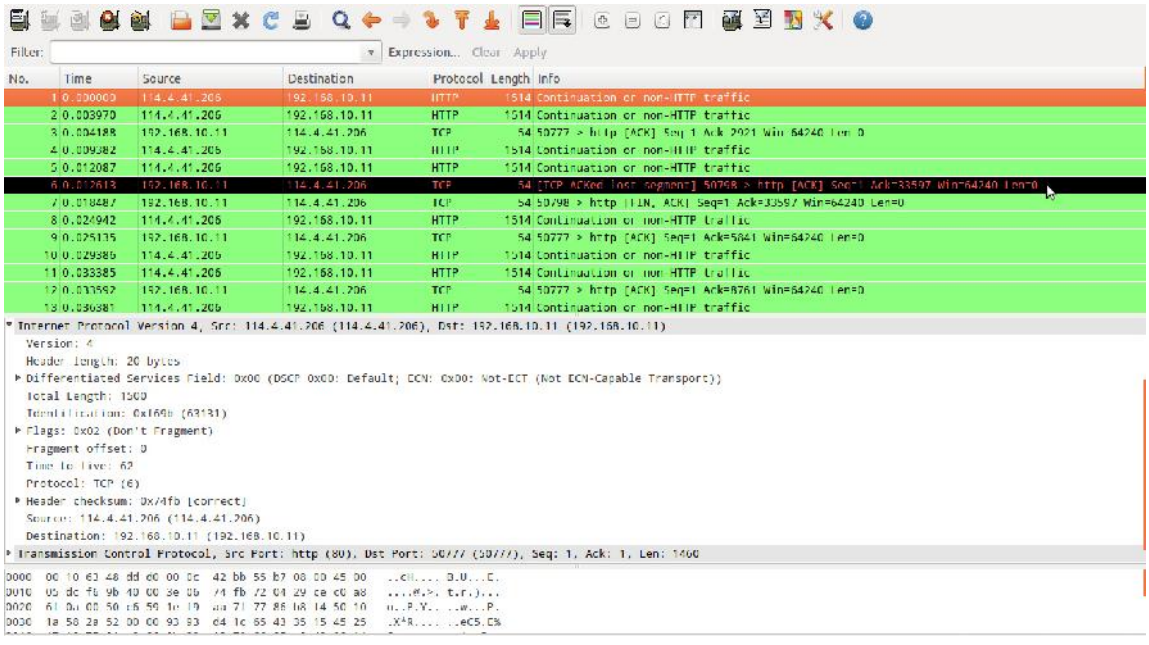


Gambar 3.13 Tampilan *Capture Interfaces*

Pada gambar 3.14 mengaktifkan *capture packets in promiscuous mode* agar wireshark dapat melakukan *capture* terhadap paket yang terdeteksi oleh *network interface card (NIC)* dari komputer dalam suatu jaringan. Setelah mengaktifkan *Capture packets in promiscuous mode* klik *start* agar wireshark mulai melakukan *sniffing* sesuai dengan konfigurasi yang dilakukan.



Gambar 3.14 Wireshark Capture Options



Gambar 3.15 Proses *sniffing* dengan *wireshark*

Gambar 3.15 merupakan tampilan *capture wireshark* saat melakukan *sniffing*. Proses ini akan berlangsung hingga waktu yang ditentukan user, Proses *sniffing* dan *capture* dengan *wireshark* tidak mempunyai batas, semakin lama melakukan *sniffing* maka semakin besar pula file yang dihasilkan.

3.7.2 Identifikasi Pengujian Jaringan

Ada beberapa poin yang dilakukan dalam pengujian jaringan yaitu sebagai berikut:

1. Melakukan konfigurasi router

   Router yang dikonfigurasi diberi akses oleh router admin berhasil dilakukan dengan baik.
2. *Packet Internet Goppher* (PING)

   PING yang dilakukan ke router admin berjalan dengan lancar tanpa adanya kesalahan.

3.7.3 Identifikasi Pengujian *Sniffing* pada Wireshark

Berikut adalah poin yang dilakukan dalam melakukan pengujian *sniffing* pada wirshark.

1. *Wireshark capture interfaces*

   Wireshark capture interfaces pada sistem operasi linux tidak bisa langsung mendeteksi *interface* yang ada pada PC, perlu penambahan beberapa baris perintah agar *interface* dapat terdeteksi oleh *wirehark.*
2. Melakukan *sniffing*

   Dalam pengujian *sniffing,* aplikasi wireshark berjalan dengan baik dan dapat menampilkan hasil penangkapan file.

Setelah melakukan pengujian sistem sesuai dengan spesifikasi alat yang digunakan, maka keluaran yang dihasilkanpun telah sesuai dengan rancangan. Untuk analisa dari hasil yang diperoleh dapat dilihat pada bab IV.

BAB IV
HASIL DAN ANALISA

4.1 Pendahuluan

Secara garis besar bab ini berisikan analisis terhadap aktivitas paket data yang terjadi ketika *client* melakukan pengunduhan. Adapun parameter yang akan di analisis pada paket data yaitu *loss packet*.

Pada analisis *loss packet* di tugas akhir ini penulis memanfaatkan *file capture* pada wireshark, pemanfaatan *file capture* pada tugas akhir ini digunakan untuk melihat lalu lintas data yang terjadi pada suatu jaringan, baik itu informasi singkat maupun detail dari suatu paket data, *statistics IO graphs* untuk menampilkan grafik dan perhitungan *loss packet*.

4.2 Analisis Paket Download

Sebuah paket data mengandung segmen data dan menyimpan informasi seperti protocol, alamat perangkat keras tujuan dan lain sebagainya. Dengan menggunakan sebuah aplikasi *network analyzer wireshark*, dapat men-*capture* segala aktivitas lalu lintas yang terjadi pada sebuah jaringan komputer saat memulai *browsing* ke sebuah alamat *Uniform Resource Locator* (URL) di internet hingga mendapatkan halaman yang diinginkan.

Metode pengambilan data sampelnya yaitu :

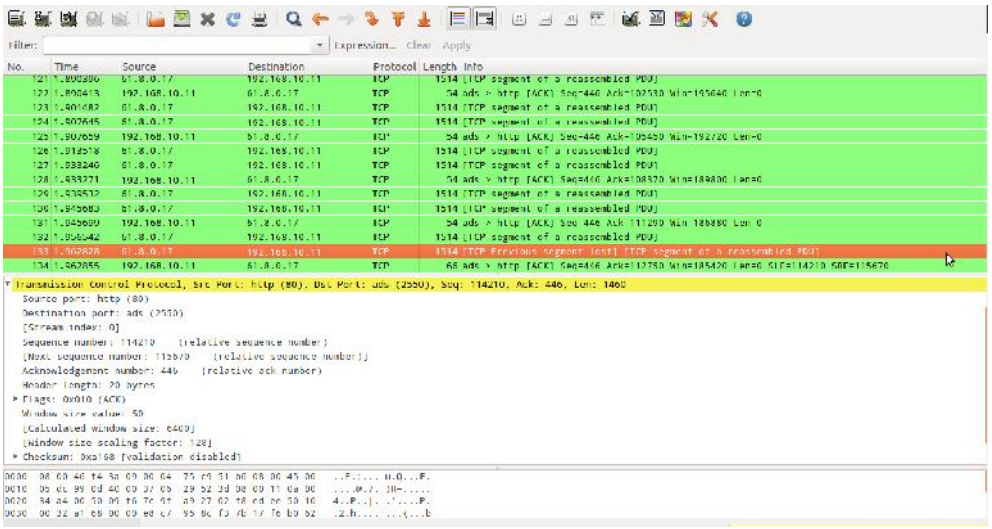
1. Waktu pengambilan data dibatasi selama 2 menit..
2. Analisis dilakukan dengan 2 tahap, yaitu :
   2.1 Pengujian download dilakukan tanpa adanya managemen bandwidth.
   2.2 Pengujian download dilakukan dengan adanya managemen bandwidth.
3. Perhitungan persentase *loss packet*.

4.3 Hasil Proses *Sniffing* dengan Wireshark

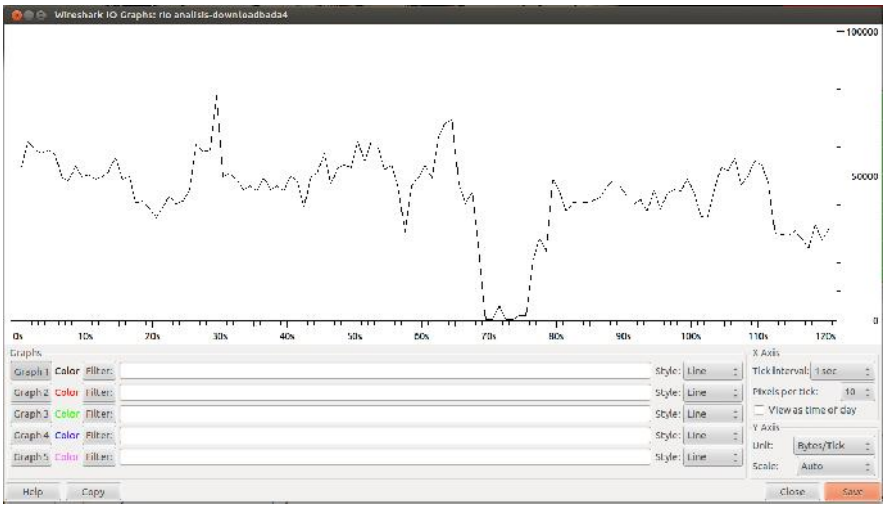
4.3.1 Percobaan Download Tanpa Managemen *Bandwidth*

Pada percobaan proses download tanpa adanya managemen *bandwidth* dilakukan pada 2 jenis percobaan, yaitu download aplikasi dari http://www.tusfiles.net/y5b1bzmvq3oq dan streaming video dari http://www.youtube.com/watch?v=gw5k6FYKMfU, masing-masing dilakukan pengulangan sebanyak 5 kali.

Pada gambar 4.1 percobaan download aplikasi terlihat adanya kehilangan segmen data sebelumnya (*previous segment lost)* pada TCP di frame 133. Pada pengamatan di frame 133 terjadi respon dari web server dengan IP 61.8.0.17 ke host 192.168.10.11 melalui port 80 menuju port 2550 dengan nomor *sequence* (*seq*): 114210 dan *acknowledgment* (*Ack*): 446 yang berarti *request* dari host sudah diterima oleh webserver dan mengalami *lost packet*.

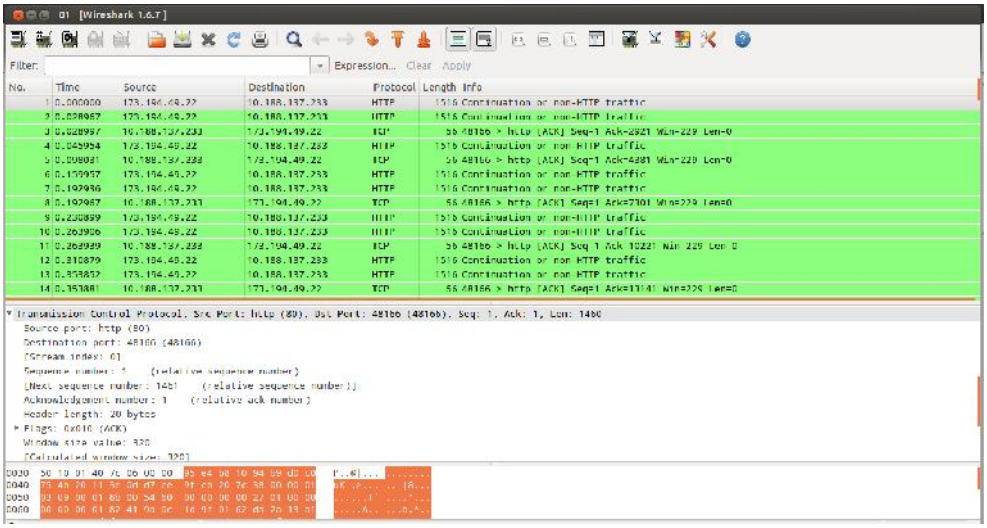


Gambar 4.1 *Capture* Proses Download Aplikasi Percobaan Tanpa Managemen *Bandwidth*

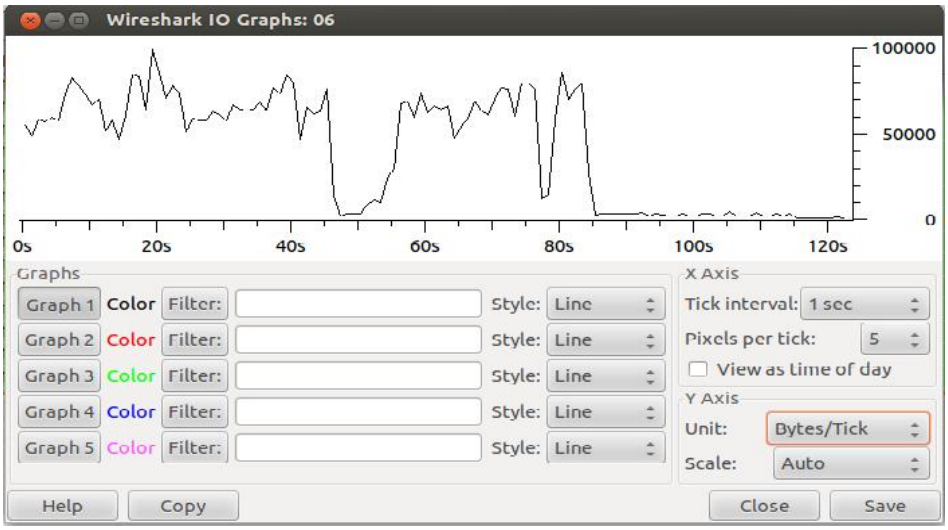


Gambar 4.2 Grafik Proses Download Aplikasi Percobaan Tanpa Managemen *Bandwidth*

Hasil *capture* percobaan streaming video yang diperoleh dari http://www.youtube.com/watch?v=gw5k6FYKMfU ditunjukkan oleh gambar 4.3 berikut ini :



Gambar 4.3 *Capture* Proses Streaming Video Percobaan Tanpa Managemen *Bandwidth*



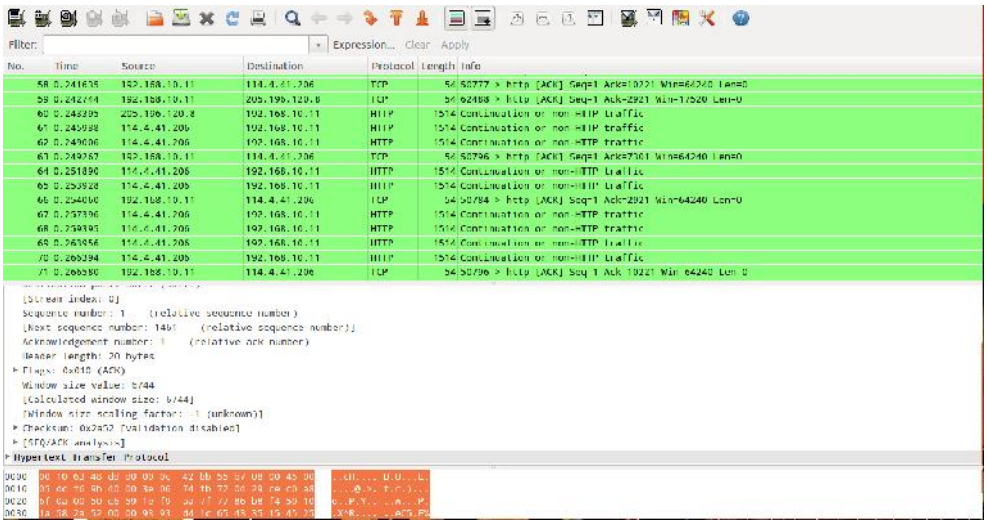
Gambar 4.4 Grafik Proses Straeming Video Percobaan Tanpa Managemen *Bandwidth*

4.3.2 Percobaan Download Menggunakan Managemen *Bandwidth*

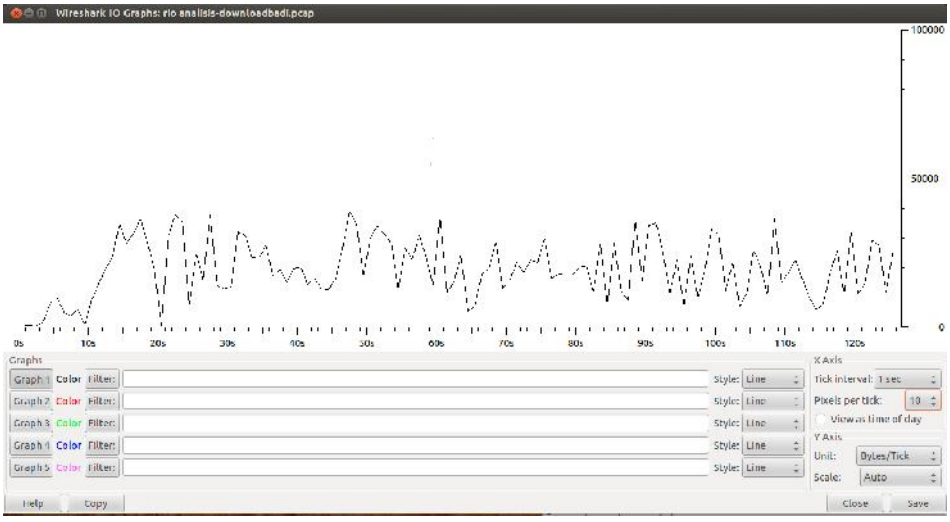
Dilakukan percobaan yang sama dengan percobaan sebelumnya, pada percobaan ini dilakukan agar mengetahui cara ini efektif untuk meminimalisir adanya *loss packet* pada suatu jaringan atau malah sebaliknya.

Pada percobaan proses download dengan adanya managemen *bandwidth* dilakukan sama dengan percobaan sebelumnya,dilakukan pada 2 jenis percobaan, yaitu download aplikasi dari http://www.tusfiles.net/y5b1bzmvq3oq dan streaming video dari http://www.youtube.com/watch?v=gw5k6FYKMfU, masing-masing dilakukan pengulangan sebanyak 5 kali.

Hasil *capture* percobaan download aplikasi yang diperoleh dari http://www.tusfiles.net/y5b1bzmvq3oq ditunjukkan oleh gambar 4.5 berikut ini :

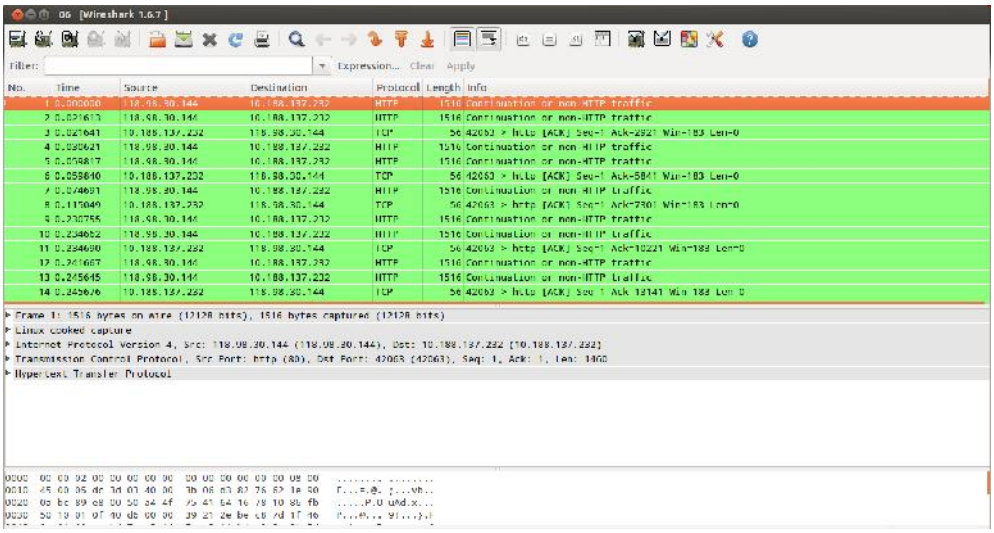


Gambar 4.5 *Capture* Proses Download Aplikasi Percobaan Menggunakan Managemen *Bandwidth*

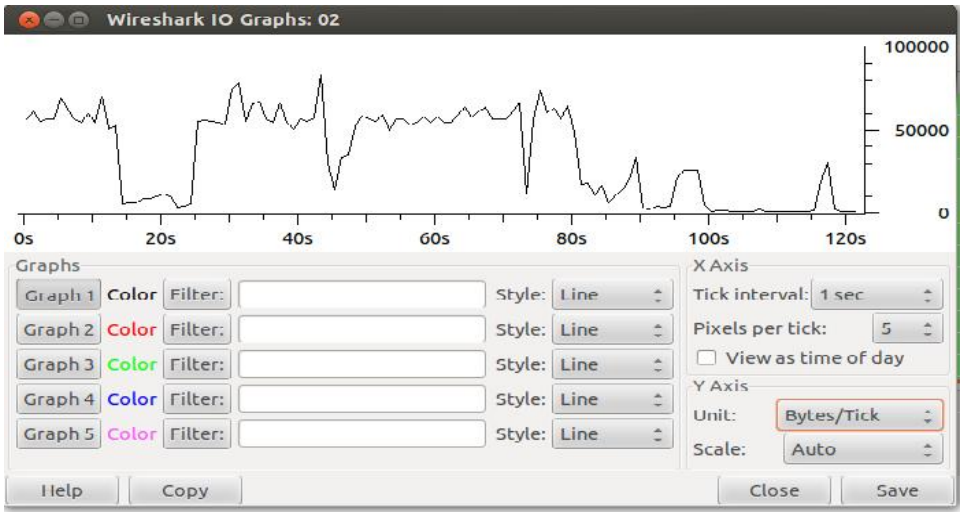


Gambar 4.6 Grafik Proses Download Aplikasi Percobaan Menggunakan Managemen *Bandwidth*

Hasil *capture* percobaan streaming video yang diperoleh dari http://www.youtube.com/watch?v=gw5k6FYKMfU ditunjukkan oleh gambar 4.7 berikut ini :



Gambar 4.7 *Capture* Proses Streamin Video Percobaan Menggunakan Managemen *Bandwidth*



Gambar 4.8 Grafik Proses Streaming Video Percobaan Menggunakan Managemen *Bandwidth*

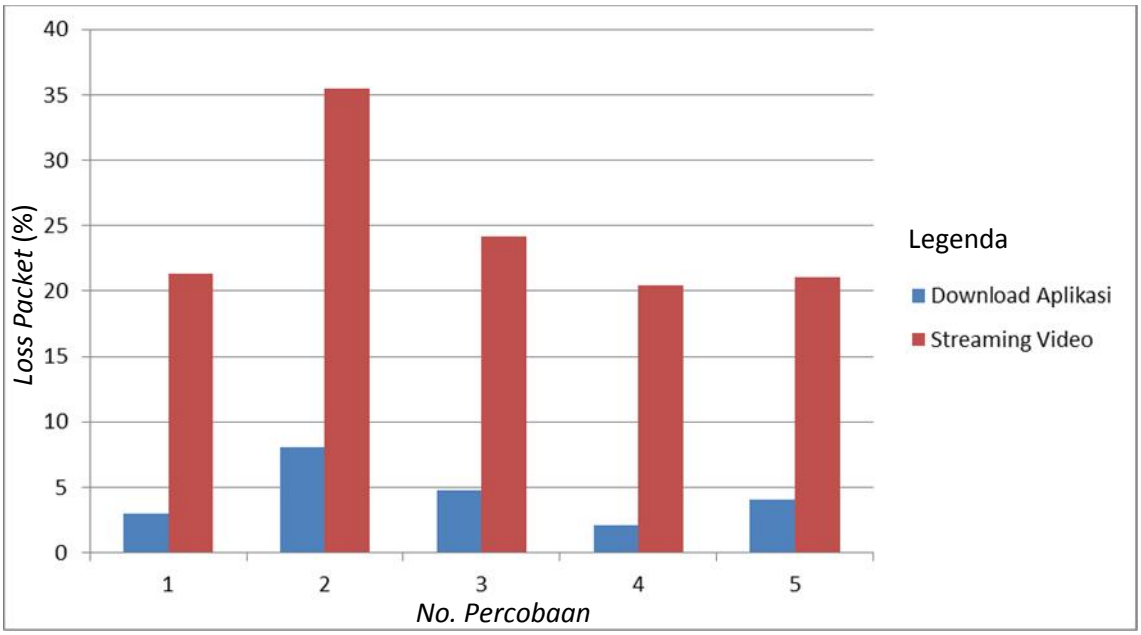
4.4 Hasil Pengujian Download

Dari *capture* data yang telah dilakukan pada wireshark maka didapatkan *loss packet* dengan cara perhitungan sebagai berikut :

Loss packet = (Paket data yang dikirim – Paket data yang diterima) x 100 %
Paket data yang dikirim

4.1 Tabel Hasil Percobaan Download Tanpa Managemen *Bandwidth*

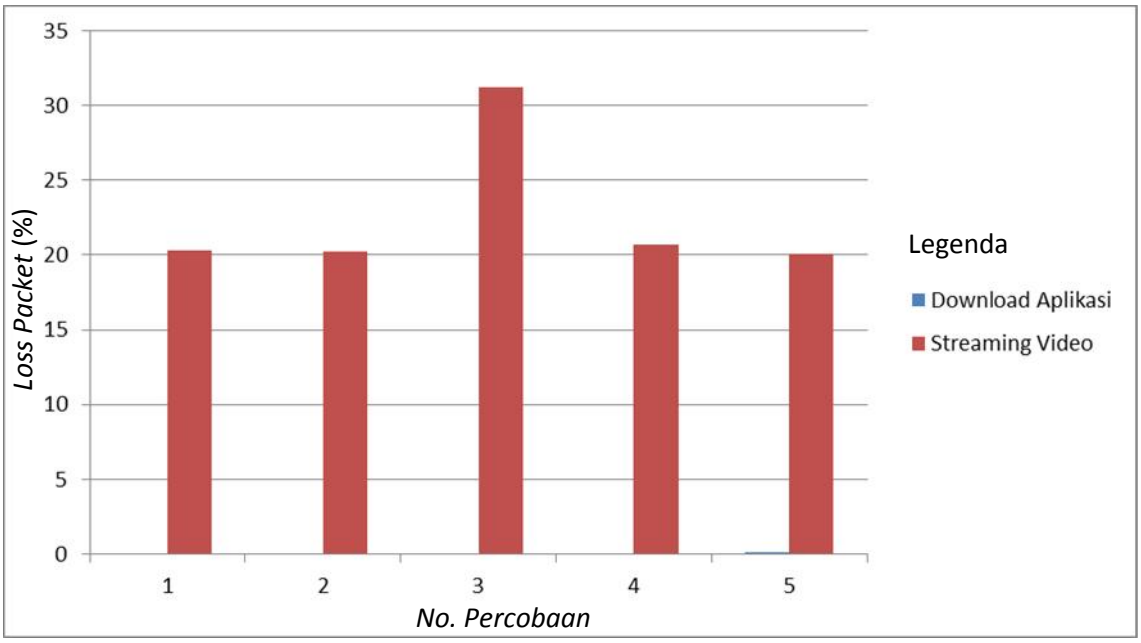
No	Tipe Percobaan	% *Loss Packet*					Rata-rata
		1	2	3	4	5	
1	Aplikasi	2,98	8,03	4,76	2,11	4,03	4,382
2	Streaming Video	21,3	35,5	24,15	20,4	21,1	24,49



Gambar 4.9 Grafik Percobaan Terhadap % *Loss Packet* Tanpa Managemen *Bandwidth*

4.2 Tabel Hasil Percobaan Download Menggunakan Managemen *Bandwidth*

No	Tipe Percobaan	% *Loss Packet*					Rata-rata
		1	2	3	4	5	
1	Aplikasi	0,02	0	0,04	0	0,16	0,044
2	Streaming Video	20,27	20,22	31,19	20,69	20,07	22,488



Gambar 4.10 Grafik Percobaan Terhadap % *Loss Packet* Menggunakan Managemen *Bandwidth*

4.5 Analisis Hasil

Berdasarkan hasil yang diperoleh dari percobaan yang telah dilakukan maka diketahui nilai rata-rata *loss packet* sebelum melakukan managemen *bandwidth* pada proses download aplikasi 4,382% dan pada streaming video 24,49%. Dilihat dari tabel *loss packet* nilai pada proses download aplikasi dan streaming video termasuk kategori jelek. Sedangkan setelah melakukan managemen *bandwidth* diperoleh nilai rata-rata pada proses download aplikasi 0,044% dan pada streaming video 22,488%. Pada tabel *loss packet* nilai pada proses download aplikasi termasuk kategori sangat bagus sedangkan pada streaming video terjadi pengurangan nilai *loss packet* tetapi masih termasuk kategori jelek. Adanya penurunan nilai *loss packet* dari penelitian ini menunjukkan bahwa dengan memanagemen *bandwidth* pada suatu jaringan dapat meminimalisir adanya *loss packet*.

BAB V
KESIMPULAN DAN SARAN

Kesimpulan dan saran yang dapat diambil dari tugas akhir yang berjudul "Analisis Loss Packet pada Proses Download di Wide Area Network menggunakan Wireshark" antara lain :

5.1 Kesimpulan

Berdasarkan parameter *loss packet* dari proses download yang dilakukan, diketahui nilai persentasi *loss packet* tanpa managemen *bandwidth* rata-rata yang diperoleh dari percobaan download aplikasi yaitu 4,328%, dan streaming video yaitu 24,49%, sedangakan pada percobaan menggunakan managemen *bandwidth* rata-rata yang diperoleh dari percobaan download aplikasi yaitu 0,044%, dan dari streaming yaitu 22,488%. Hal ini menunjukkan bahwa managemen *bandwidth* dapat meminimalisir jumlah *loss packet* sekaligus memaksimalkan kinerja suatu jaringan.

5.2 Saran

Penelitian ini berkelanjutan, dengan modal dasar ini yang perlu terus dikembangkan antara lain, menentukan konfigurasi yang tepat dengan metode yang berbeda, menganalisa dengan aplikasi yang berbeda dan melakukan beberapa perhitungan terhadap paket data yang melalui sebuah jaringan, sehingga terdapat perbandingan hasil dari penelitian yang dilakukan.

DAFTAR PUSTAKA

Handriyanto, Dwi Febrian, 2009. “Kajian Penggunaan Mikrotik Router OS Sebagai Router Pada Jaringan Komputer”. Universitas Sriwijaya. Palembang.

Taufiq, Muhammad. 2010. “CCNA Handbook Introduction to Networking. Version 2.0”. Regional Academy Cisco Networking Pasundan. Bandung.

Rafiudin, Rahmat. 2006. “Membangun Firewall dan Traffic Filtering Berbasis Cisco”. Andi Offset. Yogyakarta.

Sofana, Iwan. 2010. “Cisco CCNA dan Jaringan Komputer”. Informatika Bandung. Bandung.

Sofana, Iwan. 2008. “Membangun Jaringan Komputer untuk Pengguna Windows dan Linux”. Informatika Bandung. Bandung.

Tanenbaum, 2003. “Computer Network”. Fifth Edition. Vrije Universiteit Amsterdam, The Netherlands. http://eng.uok.ac.ir/mfathi/Courses/Computer%20Networks/Tanen/Computer%20Networks%20-%20A%20Tanenbaum%20-%205th%20edition.pdf. (Diakses : 13 juni 2013)

Forouzan, Behrouz A, 2003. “Data Communications and Networking”. Fourth Edition. DeAnza College. http://iit.qau.edu.pk/books/Data%20Communications%20and%20Networking%20By%20Behrouz%20A.Forouzan.pdf. (Diakses : 12 Juni 2013)

Haryadi, Sigit, dkk. “Pengukuran Kinerja Layanan EDGE oleh Pelanggan”. Institut Teknologi Bandung. Bandung. http://telecom.ee.itb.ac.id/~sigit/Pengukuran_kinerja_EDGE_oleh_pelanggan_SH.pdf. (Diakses : 12 Juni 2013)

http://lecturer.eepis-its.edu/~zenhadi/kuliah/Jarkom1/Prakt % 20 Modul%2014%20_analisa%20QoS.pdf. (Diakses : 13 Juni 2013)

http://lecturer.eepis-its.edu/~zenhadi/kuliah/Jarkom2/Prakt9%20Pengukuran%20QoS%20Streaming%20Server.pdf. (Diakses : 28 September 2012)

Kurniawan, Agus. 2012. “Networking Forensics Panduan Analisis dan Investigasi Paket Data Jaringan Menggunakan Wireshark”. Andi Offset. Yogyakarta.