

**PERANCANGAN BANDWIDTH ADAPTIF DENGAN
MEMANFAATKAN *INCOMING INTERNET CONTROL
MESSAGE PROTOCOL (ICMP) PACKET REQUEST***

**Tesis untuk memenuhi sebagian persyaratan
Mencapai derajat strata 2 (S2)
Program Studi Magister Sistem Informasi**



Oleh :
Rissal Efendi
J4F008023

**PROGRAM PASCA SARJANA
UNIVERSITAS DIPONEGORO
SEMARANG
2012**

ABSTRAK

Jaringan komputer merupakan kumpulan dari komputer yang melakukan komunikasi data yang membutuhkan pengaturan agar penggunaan koneksi antar jaringan dapat dilakukan secara efektif dan efisien. Pembagian *bandwidth* yang merata dibutuhkan untuk pengelolaan jaringan untuk mengakses semua sumber daya yang disediakan termasuk internet. Dalam membagi *bandwidth* secara merata dibutuhkan suatu protokol yang mampu mengidentifikasi status client yang sedang aktif. ICMP atau *Internet Control Message Protocol* merupakan protokol yang bekerja pada layer tiga yang digunakan untuk melakukan komunikasi dengan cara mengirimkan ICMP *Echo Request*. Host tujuan yang aktif akan menerima message ini dan akan mengirimkan paket ICMP *Echo Reply*. Sistem *Bandwidth* adaptif akan membagi bandwidth sama rata sehingga komputer client yang aktif akan mendapatkan porsi yang sama. Sistem *Bandwidth* adaptif akan bekerja untuk mengatur transfer data dari internet dan jaringan lokal.

Kata kunci: *bandwidth, bandwidth adaptif, internet control message protocol (ICMP).*

ABSTRACT

Computer network is a collection of computers that perform data communication that requires the setting for the use of inter-network connections can be done effectively and efficiently. Equitable distribution of bandwidth required for network management to access all the resources provided, including the Internet. The bandwidth evenly divide requires a protocol that is able to identify the current status of the client. ICMP or Internet Control Message Protocol is a protocol that works at layer three are used for communication by sending ICMP Echo Request. The active destination host receives this message and will send ICMP Echo Reply packets. Adaptive bandwidth will automatically distribute bandwidth to each active client equally and also it works to control data transfer around the internet and LAN.

Keywords: Bandwidth, Adaptive Bandwidth, Internet Control Message Protocol (ICMP)

BAB 1

PENDAHULUAN

1.1.Latar Belakang

Jaringan komputer merupakan kumpulan dari komputer yang melakukan komunikasi data yang membutuhkan pengaturan agar penggunaan koneksi antar jaringan dapat dilakukan secara efektif dan efisien. Internet sudah menjadi kebutuhan pokok suatu perusahaan atau individual dalam menjalankan bisnisnya secara *online*. Oleh karena itu, diperlukan suatu program yang dapat mengatur kecepatan bandwidth dan melakukan *monitor traffic* data di dalam jaringan.

Cara mengelola *bandwidth* juga akan mempengaruhi kelancaran distribusi *bandwidth* sehingga akan mempengaruhi kinerja. STMIK PROVISI merupakan lembaga pendidikan yang memiliki jaringan internet sebagai media untuk menunjang proses perkuliahan terutama perkuliahan yang membutuhkan internet khusus untuk melakukan Ujian online bagi mahasiswa. Selain jaringan internet, STMIK PROVISI juga memiliki jaringan komputer lokal sebagai media untuk berkomunikasi antar bagian. Dalam melakukan kegiatan perkuliahan setiap hari, internet menjadi hal yang sangat vital dalam melaksanakan kegiatan akademis, namun pada kenyataannya internet seringkali disalahgunakan untuk melakukan hal-hal yang tidak berhubungan dengan proses perkuliahan. Selama ini belum ada pembagian *bandwidth* internet secara merata di setiap bagian yang memiliki *traffic* data tinggi, sehingga pemanfaatan internet tidak dilakukan secara optimal, akibatnya kinerja setiap dosen dan mahasiswa di setiap bagian tidak dapat dilakukan secara efektif dan efisien.

Alasan tersebut menjadi ide dasar dalam penelitian tesis ini yaitu membangun sebuah aplikasi yang dapat melakukan *monitoring traffic* data pada jaringan, mengatur pembagian bandwidth yang digunakan oleh

komputer dalam jaringan secara otomatis dan merata di setiap komputer, dapat melakukan pemetaan jaringan pada komputer dalam jaringan, dapat menghasilkan *output* informasi dari *traffic* keluar masuknya data sehingga kinerja dosen dan mahasiswa yang memanfaatkan internet bisa lebih optimal.

1.2. Perumusan Masalah

Berdasarkan pada latar belakang diatas, peneliti merumuskan masalah bagaimana merancang sebuah sistem yang mampu mengirimkan ICMP packet ke semua client yang aktif kemudian mencatat IP address client-client tersebut dan mengatur alokasi *bandwidth* secara merata ke semua client.

1.3. Batasan Masalah

1. Pembagian *bandwidth* dilakukan terhadap kapasitas *bandwidth internet dan intranet*.
2. Pembagian kapasitas kecepatan *bandwidth internet* dilakukan secara merata berdasarkan pada jumlah komputer yang aktif dalam jaringan.
3. Setiap komputer *client* yang terhubung dengan komputer *server* pada jaringan harus masuk ke dalam sebuah *workgroup* yang sama.
4. Port ICMP pada komputer *client* harus dibuka sehingga bisa menerima ICMP *packet request* dari Server.
5. Uji Coba dilakukan berdasarkan kondisi nyata yang ada di Lab Cisco STMIK PROVISI Semarang.

1.4 Keaslian Penelitian

Adaptive bandwidth untuk mengatur *Quality of Service (QoS)* dijelaskan oleh Kue dan Tang (2008). Dalam skenario ini, *Adaptive Bandwidth Management* digunakan untuk mengatur lalu lintas data untuk mengatur prioritas data dalam *Quality of Service* terutama dalam jaringan *Ad Hoc* yang berskala luas. Pada penelitian ini Kue dan Tang sebelumnya mengatur jenis data yang akan mendapat prioritas untuk dikirimkan

melalui jaringan ad hoc yang relatif mempunyai bandwidth yang terbatas dibanding dengan jaringan *wireless* lainnya. Jaringan *Ad hoc* yang merupakan jaringan *point-to-point* antar *end user* yang menjadi alternatif dalam komunikasi data untuk mengirimkan dan menerima data yang terbatas.

Adaptive Bandwidth Sharing untuk mengatur jaringan dengan skala besar dijelaskan juga oleh Tamura dan Tobe (2009). Dalam penelitian ini Tamura dan Tobe menggunakan *Neighbor State based Queuing* untuk memperbaiki kinerja pendistribusian bandwidth pada shared link yang akan dilewati oleh berbagai macam paket data dengan menggunakan protokol yang berbeda-beda. *Adaptive bandwidth* ini bekerja pada router berdasarkan pada status yang diterima oleh link dengan cara menerima informasi dari *neighbor* yang sedang menerima dan memproses paket data.

Adaptive bandwidth juga digunakan untuk memperbaiki kinerja dari jenis paket data yang akan dilewatkan melalui server. Pada penelitian ini Feilin dan Xue (2008) menggunakan *Improve dynamic Priority Queue* untuk komunikasi data pada Multimedia. *Adaptive bandwidth* ini bekerja dengan cara memilih jenis paket data yang akan mendapatkan prioritas untuk diteruskan ke *client*.

Penelitian yang dilakukan adalah merancang sebuah sistem yang mampu membagi *bandwidth* ke semua client yang aktif dengan memanfaatkan *ICMP Packet Request*. Perbedaan antara sistem yang dibuat dengan penelitian-penelitian yang lain adalah sistem ini mampu membagi bandwidth sama rata ke semua client yang mampu membagi bandwidth internet maupun *bandwidth* dalam satu jaringan komputer. Sistem ini bekerja pada lapisan dua data link pada OSI 7 Layers. Pembagian bandwidth didasarkan pada jumlah IP address yang aktif yang kemudian dipetakan ke MAC address. Sistem ini juga bisa dipasang pada server

lokal yang membutuhkan pengelolaan bandwidth sehingga semua client yang merequest packet akan mendapatkan porsi yang sama.

1.5 Manfaat Penelitian

Pada penelitian ini, manfaat yang ingin dicapai adalah:

1. Memberikan kemudahan bagi administrator jaringan dalam mengelola bandwidth tanpa harus melakukan konfigurasi terlebih dahulu.
2. Menghemat penggunaan peralatan jaringan untuk melakukan manajemen bandwidth.
3. Menghemat penggunaan PC Server yang digunakan untuk manajemen bandwidth.
4. Meningkatkan kinerja dosen yang membutuhkan koneksi internet.
5. Meningkatkan kinerja mahasiswa yang sedang melakukan ujian *on-line*.

1.6 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Memberikan kemudahan dalam mengelola bandwidth yang dialokasikan ke semua komputer yang aktif.
2. Menghindari pemakaian *bandwidth* yang ekstrim oleh sejumlah *user*
3. Mengatur alokasi *bandwidth* dalam jaringan komputer secara merata.
4. Menghasilkan sistem yang mampu mengatur banyaknya alokasi bandwidth internet secara otomatis berdasarkan pada jumlah komputer yang aktif.
5. Melihat banyaknya *traffic* data dalam jaringan
6. Melakukan pemetaan jaringan bagi komputer server dan *client* yang aktif.

BAB 2

LANDASAN TEORI

2.1 Tinjauan Pustaka

Pada publikasi yang dilakukan oleh Laurent (1998) *Adaptive Bandwidth* adalah suatu metode pengalokasian *bandwidth* atau *data transfer rate* secara otomatis berdasarkan tingkat kebutuhan *bandwidth* pada jaringan agar dapat meningkatkan *Quality of Service* (QoS). Konsep *Adaptive Bandwidth* memiliki dua jenis, yaitu *Adaptive Bandwidth* yang membagi *bandwidth* berdasarkan tingkat kebutuhan pengguna dan *Adaptive Bandwidth* yang membagi *bandwidth* secara merata untuk setiap pengguna. Dalam publikasinya, *Adaptive Bandwidth* berdasarkan tingkat kebutuhan pengguna belum dapat diterapkan secara maksimal karena dengan spesifikasi komputer yang berbeda-beda dalam jaringan, akan mempengaruhi pembagian *bandwidth* apabila terdapat komputer dengan spesifikasi mesin yang lebih tinggi, akibatnya komputer dengan spesifikasi mesin yang lebih rendah akan diabaikan kebutuhan *bandwidth*nya. Sedangkan *Adaptive Bandwidth* yang membagi *bandwidth* secara merata dapat diterapkan lebih optimal karena pembagian *bandwidth* ini mengabaikan spesifikasi mesin komputer yang terdapat dalam jaringan.

Penelitian tentang *Adaptive Bandwidth* yang dilakukan oleh Xu, Tang dan Bagrodia (2008) menjelaskan bahwa *bandwidth* adaptif adalah cara mengatur bandwidth sesuai dengan kebutuhan user dan jenis aplikasi yang diperbolehkan untuk memakai *bandwidth* adaptif tersebut. Dalam publikasinya yang berjudul *Adaptive Bandwidth Management and Quality of Service Provisioning in Large Scale Ad Hoc Networks*, *bandwidth* adaptif mengatur lalu lintas data yang terjadi pada jaringan *Ad hoc*. Pada penelitian yang dilakukan, *bandwidth* adaptif diterapkan pada jaringan yang lebih luas dengan jumlah host yang tersebar di tempat yang berbeda. Penerapan *bandwidth* adaptif pada skala yang lebih luas dihasilkan *data transfer rate* yang lebih sedikit karena *delay* yang dibutuhkan untuk mengirimkan data menjadi lebih lama. Sedangkan pada skala yang lebih sempit dihasilkan *data transfer rate* yang lebih besar karena *delay* yang dibutuhkan lebih cepat.

Pada publikasi Lamle (2000), ICMP merupakan protokol yang digunakan untuk melakukan tes koneksi dari sebuah host ke host yang lain. ICMP melakukan tes koneksi dengan mengirimkan sebuah request packet ke host tujuan dengan menggunakan IP address. ICMP merupakan protokol pesan pada TCP/IP. ICMP menyediakan pesan *control* dan *error* yang digunakan oleh ping dan traceroute yang bekerja pada layer jaringan. Pesan ICMP yang bisa dikirim dari satu host ke host yang lain adalah:

1. *Host Confirmation.*

ICMP Echo Message dimanfaatkan untuk mengirimkan pesan untuk memastikan apakah host tujuan sedang aktif atau tidak. Host tujuan akan menerima pesan tersebut dan akan mengirimkan paket *ICMP Echo Reply*.

2. *Unreachable Destination or Service*

ICMP Destination Unreachable bisa digunakan untuk memberitahu sebuah host bahwa host yang dituju tidak dalam satu jaringan dan tidak bisa dijangkau karena tidak ada rute untuk mengirimkan data. Ketika sebuah host atau gateway menerima paket untuk diteruskan ke sebuah host yang tidak terjangkau, maka gateway akan mengirimkan sebuah *ICMP Destination Unreachable* ke host asal. Paket *Destination unreachable* berisi kode yang merupakan indikasi bahwa paket tidak bisa dikirimkan. Kode-kode tersebut antara lain:

0 = *network unreachable* : merupakan respon yang dikirimkan oleh router yang tidak mampu meneruskan paket karena tidak menemukan rute menuju ke tujuan pada *routing table*.

1 = *host unreachable* : merupakan respon yang dikirimkan oleh router yang menemukan network tujuan pada *routing table* namun tidak menemukan host pada network tersebut.

2 = *protocol unreachable* : merupakan respon yang dikirimkan oleh host tujuan yang mengindikasikan bahwa TCP segment atau UDP Segment dalam sebuah paket tidak bisa dikirimkan ke layer selanjutnya.

3 = *port unreachable*: merupakan respon yang dikirimkan oleh host tujuan bahwa *port* atau *service* tidak aktif.

3. *Time Exceeded*

Pesan *Time exceeded* digunakan untuk mengindikasikan bahwa sebuah paket tidak bisa dikirimkan karena waktu pengiriman (*time to live*) sudah habis. *Time to live* merupakan waktu yang disediakan untuk mengirim paket sampai ke tujuan, jika waktu habis sebelum paket sampai ke tujuan maka paket akan dibuang.

4. *Route Redirection*

Route Redirection merupakan pesan yang dikirimkan ke host dalam jaringan yang memberitahu bahwa terdapat rute yang lebih baik untuk mengirimkan data.

5. *Source quench*

ICMP *Source Quench* message merupakan pesan yang dikirimkan oleh router yang memberitahu host pengirim untuk menghentikan pengiriman paket karena router mempunyai *buffer* yang terbatas..

Berdasarkan pada tinjauan pustaka diatas bahwa fungsi dari protocol ICMP adalah untuk mengetahui bahwa host dalam jaringan aktif maka peneliti berkeinginan untuk merancang sebuah sistem yang mampu membagi *bandwidth* secara otomatis sesuai dengan jumlah komputer client yang aktif dengan memanfaatkan *Internet Control Message Control Protocol (ICMP) packet request*.

2.2 Landasan Teori

Jaringan komputer merupakan sebuah kumpulan komputer baik yang bertindak sebagai server maupun client yang terhubung melalui media dan alata jaringan. Jaringan komputer dibangun dengan tujuan untuk melakukan komunikasi data antar komputer di jaringan tersebut. Selain itu tujuan dari dibangunnya jaringan komputer adalah untuk berbagi sumber daya antar dua komputer yang berbeda.

Monitoring atau pengawasan adalah proses dalam menetapkan ukuran kinerja dan pengambilan tindakan yang dapat mendukung pencapaian hasil yang diharapkan sesuai dengan kinerja yang telah ditetapkan tersebut. *Network monitoring* adalah suatu proses pengawasan dan segala tindakan yang dilakukan didalam manajemen sebuah jaringan komputer agar dapat menghasilkan kinerja yang sesuai, efektif dan efisien (Nyirenda, dkk, 2002).

Dalam melakukan tugasnya, administrator jaringan juga bertindak sebagai pengawas untuk mengawasi keluar masuknya data dalam jaringan, menjaga supaya *traffic* data dalam jaringan selalu konsisten dalam segi keamanan dan kesinkronan data.

2.2.1. Simple Network Management Protocol (SNMP)

SNMP adalah sebuah protokol yang dirancang untuk memberikan kemampuan kepada pengguna untuk memantau dan mengatur jaringan komputernya secara sistematis dari jarak jauh atau dalam satu pusat kontrol saja. Pengolahan ini dijalankan dengan mengumpulkan data dan melakukan penetapan

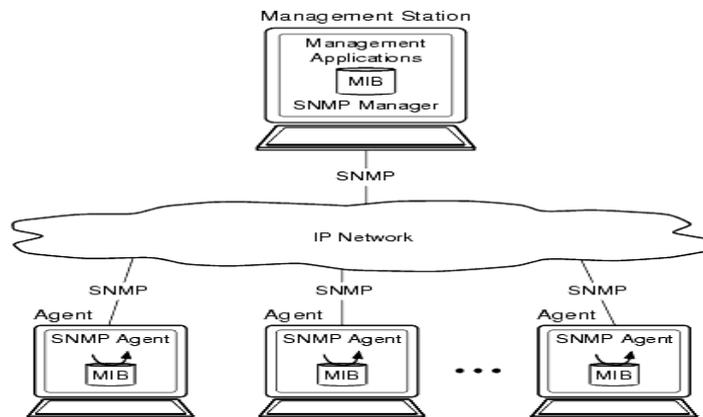
terhadap variabel-variabel dalam elemen jaringan yang dikelola. *Simple Network Management Protocol* (SNMP) merupakan protokol standard industri yang digunakan untuk memonitor dan mengelola berbagai perangkat di jaringan Internet meliputi *hub, router, switch, workstation* dan sistem manajemen jaringan secara jarak jauh (*remote*). Secara umum SNMP dapat didefinisikan sebagai aturan yang menghubungkan antara dua tipe objek SNMP yaitu SNMP manager dan SNMP agen. SNMP dapat digunakan untuk *remote monitoring* dan *network traffic control*.

SNMP didesain untuk mengurangi tingkat kompleksitas dari manajemen jaringan dan banyaknya sumber daya yang dibutuhkan untuk mendukung manajemen tersebut. Adanya SNMP memungkinkan manajemen jaringan yang tersentralisasi, kuat, dan kompatibel pada semua platform. Selain itu, SNMP memberikan fleksibilitas untuk manajemen informasi-informasi yang dimiliki oleh vendor produk tertentu (Nugraha, 2007).

SNMP dikembangkan untuk menyediakan sistem manajemen jaringan yang mendasar dan mudah diterapkan bagi rangkaian protokol seperti TCP/IP. Ini mencakup suatu kerangka kerja operasi dan representasi informasi manajemen. *Structure of Management Information* (SMI) memungkinkan terdefinisinya *Management Information Base* (MIB). MIB dapat dianalogikan dengan skema database, bagi yang sudah terbiasa dengan definisi basis data dan juga merupakan sebuah entitas terarah yang dikenal sebagai agent (Afdhal dan Gani, 2005).

Komponen utama SNMP ada dua, yaitu *SNMP agent* dan *SNMP manager*. SNMP agen mampu mengirimkan informasi secara mendadak kepada SNMP

manager pada situasi-situasi tertentu. Sedangkan *SNMP manager* digunakan untuk memantau keadaan jaringan dengan meminta data kepada *SNMP agen* dalam bentuk *request* dan *response*.



Gambar 2.1 Komponen SNMP

SNMP agen adalah suatu perangkat lunak jaringan komputer yang dijalankan pada elemen jaringan *SNMP* yang akan dikelola. *SNMP agen* ini meminta respon dari protokol *SNMP* dari sebuah *SNMP manager*. Kemudian agen-agen tersebut diarahkan pada sistem hardware jaringan seperti *PC*, *Router*, *Switch*, *Repeater* dan sistem *hardware* yang lainnya yang membutuhkan adanya manajemen.

SNMP manager merupakan platform sistem manajemen atau pelaksana dari manajemen jaringan. Pada kenyataannya *SNMP manager* ini merupakan komputer biasa yang ada pada jaringan yang mengoperasikan perangkat lunak untuk manajemen jaringan. *SNMP manager* ini terdiri atas satu proses atau lebih yang berkomunikasi dengan agen-agenya dan berfungsi untuk mengumpulkan

informasi dari agen dalam jaringan. *SNMP manager* akan mengumpulkan informasi dari jaringan yang diminta oleh *administrator* saja dan bukan semua informasi yang dimiliki oleh agen (Afdhal dan Gani, 2005).

2.2.2. *Bandwidth*

Bandwidth adalah luas atau lebar frekuensi yang digunakan oleh sinyal dalam medium transmisi. *Bandwidth* sering digunakan sebagai suatu sinonim untuk *data transfer rate* yaitu jumlah data yang dapat dibawa dari sebuah titik ke titik lain dalam jangka waktu tertentu. Jenis *bandwidth* ini biasanya diukur dalam satuan kecepatan bps (bits per second) dan Kbps (Kilobits per second).

2.2.3. *Network Mapping*

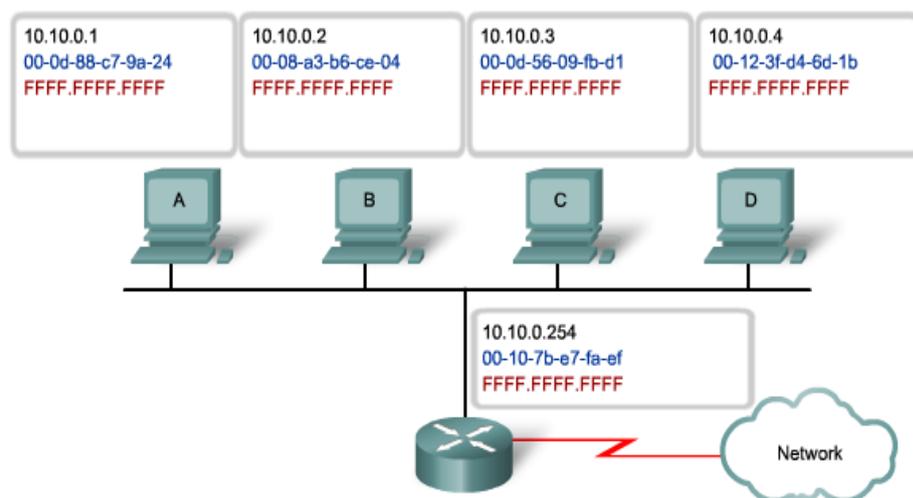
Network Mapping atau NMAP adalah suatu penggambaran operasionalitas sebuah jaringan yang akan menghasilkan data NMAP berupa penggambaran komputer yang masih aktif dalam jaringan maupun komputer yang sudah tidak aktif dalam jaringan (offline). Proses NMAP akan melakukan scan komputer-komputer yang aktif dalam jaringan dan services. Hasil scanning komputer berupa daftar port yang aktif, sedangkan hasil scanning komputer yang aktif akan menampilkan daftar komputer yang sedang aktif atau up dan daftar komputer yang sedang tidak aktif atau down (Adipranata, 2004).

2.2.4. *Address Resolution Protocol (ARP)*

Address Resolution Protocol (ARP) adalah sebuah protokol dalam *TCP/IP Protocol Suite* yang bertanggungjawab dalam melakukan resolusi alamat IP ke dalam alamat *Media Access Control (MAC)* address. ARP didefinisikan didalam *Request for Comment (RFC) 826*.

Sebuah komputer dalam jaringan membutuhkan dua alamat untuk dapat melakukan komunikasi data dengan komputer yang lain. Alamat tersebut adalah *physical address* dan *logical address*. *Physical address* adalah alamat fisik suatu komputer yang bersifat permanen yang tersimpan dalam *Network Interface Card* (NIC). Sedangkan *Logical Address* adalah alamat *Internet Protocol* (IP) yang bisa diubah sesuai dengan kebutuhan user. Sebuah aplikasi yang mendukung protokol jaringan TCP/IP mencoba untuk mengakses sebuah host TCP/IP dengan menggunakan alamat *Internet Protocol* (IP), maka alamat IP tersebut harus diterjemahkan kedalam MAC address.

ARP akan melakukan broadcast terhadap sebuah *ARP Request Packet*. Broadcast akan dilakukan ke semua komputer yang aktif untuk menemukan *MAC address* dari *IP address* yang dituju. Host yang melakukan permintaan selanjutnya menyimpan pemetaan alamat *IP* dan *MAC* didalam *Local ARP cache* secara sementara, sehingga dapat diakses lain waktu tanpa harus mengirimkan *broadcast* lagi (Todd Lamle,2000).



Gambar. 2.3 Address Resolution Protocol (ARP)

Host yang mengirimkan *broadcast* diluar jaringan lokal, maka ARP akan mencoba untuk mendapatkan *MAC Address* dari antarmuka *router local* sebagai gateway yang menjadi jembatan antar jaringan yang berbeda.

2.2.5. Service Port

Port bisa dikatakan sebagai jalan atau lorong yang menghubungkan antar beberapa host agar dapat saling berkomunikasi. Service atau layanan dalam berkomunikasi selalu menggunakan port-nya masing-masing. Dari nomor port yang terdiri atas 0 sampai 65535 terdapat beberapa *service port* yang berfungsi sebagai remote login.

Tabel 2.4 Port yang dipakai pada Internet

Port	Keterangan
21	File Transfer Protokol
22	Secure Shell
23	Telnet
25	SMTP
80	HTTP (WWW)
194	Protokol IRC
1080	SOCKS (proxy IRC)

2.2.6. TCP / IP

TCP (*Transmission Control Protocol*) melayani servis pengiriman data yang reliable. Data dijamin utuh sampai di tujuan, jika transmisi terganggu maka data akan terus dikirim ulang.

IP (*Internet Protocol*) melayani servis pengiriman data yang unreliable. Data dikirim tanpa ada jaminan akan keutuhannya, bahkan sampai atau tidak sampai IP tidak peduli. Berikut lapisan-lapisan pada protocol TCP/IP : dimana pada lapisan aplikasi (meringkas lapisan aplikasi, presentasi, sesi) dan Network (physical, data link, network)



Gambar 2.5 Lapisan Protokol TCP/IP

Di luar protokol tadi, apapun masalahnya, kenyataannya jaringan komputer tidak akan mampu dikelola tanpa adanya pengalamatan. Tipe alamat yang digunakan pada jaringan ada macam-macam, ada *MAC Address*, *IP Address*, *IPX Network Address*, dan lain-lain.

Bagi para pengguna LAN perlu mengenal *hostname* dari mesin yang dituju, seperti : *server.indo.net. id*, *rad.net.id*, *ui.ac.id*, *itb.ac.id*. Bagi komputer untuk bekerja langsung menggunakan informasi tersebut akan relatif lebih sulit karena

tidak ada keteraturan yang dapat di programkan dengan mudah. Untuk mengatasi hal tersebut, komputer mengidentifikasi alamat setiap komputer menggunakan sekumpulan angka sebanyak 32 bit yang dikenal sebagai IP address. Seluruh host (komputer) yang terhubung ke Internet dan ingin berkomunikasi memakai TCP/IP harus memiliki IP Address sebagai alat pengenalan host pada network.

Secara logika, Internet merupakan suatu *network* besar yang terdiri dari berbagai sub network yang terintegrasi. Oleh karena itu, suatu IP Address harus bersifat unik untuk seluruh dunia. Di internet, IP address digunakan untuk memberikan alamat suatu server, situs (*web server*), alat (*router, network card*), bahkan yang terbaru (IPv6) dapat digunakan untuk pengalamatan alat-alat elektronik terintegrasi jaringan (mesin, mobil, perabot rumah tangga).

Transmission Control Protocol (TCP) mempunyai beberapa karakteristik sebagai berikut:

1. *Connection-oriented* : Sebelum data dapat ditransmisikan antara dua *host*, dua proses yang berjalan pada lapisan aplikasi harus melakukan negosiasi untuk membuat sesi koneksi terlebih dahulu. Koneksi TCP ditutup dengan menggunakan proses terminasi koneksi TCP (*TCP connection termination*).
2. *Full-duplex*: Untuk setiap host TCP, koneksi yang terjadi antara dua host terdiri atas dua buah jalur, yakni jalur keluar dan jalur masuk. Dengan menggunakan teknologi lapisan yang lebih rendah yang mendukung *full-duplex*, maka data dapat secara simultan diterima dan dikirim. *Header* TCP berisi nomor urut (*TCP sequence number*) dari data yang ditransmisikan dan sebuah *acknowledgment* dari data yang masuk.

3. *Reliable*: Data yang dikirimkan ke sebuah koneksi TCP akan diurutkan dengan sebuah nomor urut paket dan akan mengharapkan paket *positive acknowledgment* dari penerima. Jika tidak ada paket *Acknowledgment* dari penerima, maka segmen TCP (*protocol data unit* dalam protokol TCP) akan ditransmisikan ulang. Pada pihak penerima, segmen-segmen duplikat akan diabaikan dan segmen-segmen yang datang tidak sesuai dengan urutannya akan diletakkan di belakang untuk mengurutkan segmen-segmen TCP. Untuk menjamin integritas setiap segmen TCP, TCP mengimplementasikan penghitungan *TCP Checksum*.

4. *Byte stream*: TCP melihat data yang dikirimkan dan diterima melalui dua jalur masuk dan jalur keluar TCP sebagai sebuah *byte stream* yang berdekatan (kontigu). Nomor urut TCP dan nomor *acknowledgment* dalam setiap header TCP didefinisikan juga dalam bentuk *byte*. Meski demikian, TCP tidak mengetahui batasan pesan-pesan di dalam *byte stream* TCP tersebut. Untuk melakukannya, hal ini diserahkan kepada protokol lapisan aplikasi (dalam DARPA Reference Model).

5. *Flow control*: Untuk mencegah data terlalu banyak dikirimkan pada satu waktu, yang membuat *congestion* jaringan *internetwork* IP, TCP mengimplementasikan layanan *flow control* yang dimiliki oleh pihak pengirim yang secara terus menerus memantau dan membatasi jumlah data yang dikirimkan pada satu waktu. Untuk mencegah pihak penerima untuk memperoleh data yang tidak dapat disangganya (buffer), TCP juga mengimplementasikan *flow control*

dalam pihak penerima, yang mengindikasikan jumlah *buffer* yang masih tersedia dalam pihak penerima.

6. Melakukan segmentasi terhadap data yang datang dari lapisan aplikasi (dalam *DARPA Reference Model*)

7. Mengirimkan paket secara "*one-to-one*": hal ini karena memang TCP harus membuat sebuah sirkuit logis antara dua buah protokol lapisan aplikasi agar saling dapat berkomunikasi. TCP tidak menyediakan layanan pengiriman data secara *one-to-many*.

2.2.7. Internet Protocol Address

Sofana (2010 : 255) menjelaskan bahwa *Internet Protocol* (IP) merupakan sebuah protokol yang terletak pada *layer* atau lapisan *Internet/Network*. IP merupakan protokol yang bersifat *connectionless* dan *unreliable* serta merupakan inti dari protokol TCP/IP. *Connectionless* mempunyai arti bahwa IP tidak perlu membuat dan memelihara sebuah sesi koneksi, sedangkan *unreliable* mempunyai arti bahwa protokol ini tidak menjamin penyampaian paket data tapi diserahkan kepada protokol pada lapisan yang lebih tinggi yakni *Transmission Control Protocol* (TCP). IP mempunyai *header* yang terdapat *field* berisi informasi *internet address* atau *IP Address*. *IP Address* memuat informasi berupa alamat asal dan tujuan dari paket data.

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
Version				IHL				TOS/DSCP/ECN				Total Length																											
Identification										Flags				Fragment Offset																									
Time To Live				Protocol				Header Checksum																															
Source Address																																							
Destination Address																																							
Options																								Padding															

Gambar 2.6 Header Protokol IP
(sumber : Sofana, 2010 : 256)

Sofana (2010 : 258) menjelaskan bahwa *IP address* merupakan identifikasi setiap *host* pada sebuah jaringan komputer, baik intranet maupun *internet*. Setiap *host* atau komputer yang terhubung dalam sebuah jaringan harus memiliki nomor identifikasi unik berupa *IP address* agar dapat menjadi pembeda dengan *host* atau komputer lain, artinya setiap *host* atau komputer tidak boleh menggunakan *IP address* yang sama.

IP address merupakan sekumpulan bilangan biner sepanjang 32 *bit*, yang dibagi atas 4 bagian dimana setiap bagian mempunyai panjang 8 *bit*. *IP address* memiliki penulisan yang dikenal dengan notasi “*dotted decimal*”, penulisan secara desimal yang digunakan sebagai alamat *host*. Contoh penulisan *IP address* sebagai berikut :

Tabel 2.1 Penulisan IP Address

Bilangan Biner
01000100 10000001 11111111 00000001

Bilangan Desimal
68.129.255.1

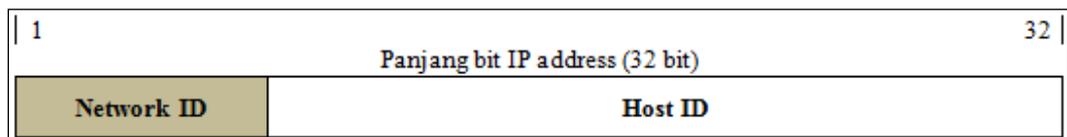
(sumber : Sofana, 2010 : 259)

Alokasi penggunaan IP *address* di berbagai negara diatur oleh sebuah lembaga yang bernama *Internet Assigned Numbers Authority* (IANA). Alokasi IP *address* tidak semuanya digunakan untuk keperluan alamat *host*, namun ada yang digunakan untuk keperluan khusus seperti untuk keperluan alamat *network*, alamat *broadcast*, alamat *localhost*, LAN, dan sebagainya. IANA mencadangkan beberapa IP *address* berikut untuk jaringan intranet atau LAN :

1. Dimulai dari bilangan 10. (10.0.0.0 sampai 10.255.255.255)
2. Dimulai dengan bilangan 127.
3. Dimulai dengan bilangan 169.254.
4. Dimulai dengan bilangan 172.16. sampai 172.31.
5. Dimulai dengan bilangan 192.168.

IP *address* mempunyai 5 buah kelas yaitu kelas A, B, C, D, E, namun dalam penggunaannya, hanya kelas A, B, dan C yang digunakan untuk keperluan publik atau umum. IP *address* kelas A, B, dan C disebut IP *address unicast*. IP *address* kelas D dan E digunakan untuk keperluan khusus. IP *address* kelas D disebut juga IP *address multicast*, sedangkan kelas E digunakan untuk keperluan riset.

IP address kelas A, B, dan C dapat dipisahkan menjadi 2 bagian, yakni bagian *network* (*bit-bit network/network bits*) dan bagian *host* (*bit-bit host/host bits*). *Network bits* mempunyai peran sebagai pembeda antar *network* atau identifikasi ID *network*, sedangkan *host bits* berperan sebagai identifikasi ID *host*. Semua *host* yang terhubung pada *network* yang sama memiliki *network bits* yang sama juga.



Gambar 2.7 Network ID dan Host ID

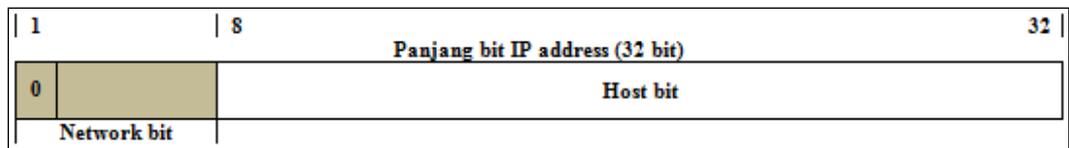
(sumber : Sofana, 2010 : 262)

Menurut Sofana (2010 : 262), perbedaan *network* pada jaringan TCP/IP tidak ditentukan oleh perbedaan topologi, media fisik jaringan, kontrol akses, sistem operasi, dan aplikasi. Jika ada dua buah jaringan menggunakan topologi yang berbeda namun *network bit* keduanya sama, maka kedua jaringan tersebut bisa dikatakan berada pada satu *network*. Sebaliknya, apabila sebuah *host* memiliki *network bit* yang berbeda dengan *host* lain walaupun berada pada topologi yang sama, maka *host* tersebut berbeda *network* dengan *host* yang lain.

A. IP Address Kelas A

Bit pertama pada kelas A mempunyai nilai 0. *Bit* ini dan 7 *bit* berikutnya (8 *bit* pertama) merupakan *bit-bit network* (*network bit*) dan boleh bernilai berapa saja (kombinasi angka 1 dan 0). Sedangkan sisa 24 *bit* terakhir merupakan *bit-bit*

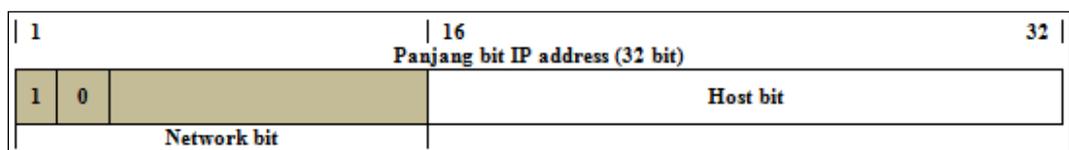
untuk *host*. Penulisan bilangan biner untuk kelas A dapat dituliskan sebagai : **nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh** (n menyatakan *network*, sedangkan h menyatakan *host*).



Gambar 2.3 IP address kelas A
(sumber : Sofana, 2010 : 263)

B. IP Address Kelas B

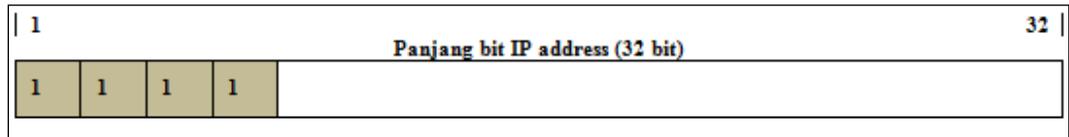
Dua *bit* pertama kelas B bernilai 10. Dua *bit* ini dan 14 *bit* berikutnya (16 *bit* pertama) merupakan *bit network* dan boleh bernilai berapa saja dengan kombinasi angka 1 dan 0. Sedangkan sisa 16 *bit* terakhir merupakan *bit-bit host*. IP address kelas B dapat dituliskan sebagai : **nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh** (n menyatakan *network*, sedangkan h menyatakan *host*).



Gambar 2.8 IP address kelas B
(sumber : Sofana, 2010 : 264)

C. IP Address Kelas C

Tiga *bit* pertama bernilai 110. Tiga *bit* ini dan 21 *bit* berikutnya (24 *bit* pertama) merupakan *bit network* dan boleh bernilai berapa saja dengan kombinasi



Gambar 2.11 IP address kelas E
(sumber : Sofana, 2010 : 265)

2.2.8. Private IP Address

Private IP address merupakan IP address yang digunakan untuk keperluan dalam jaringan lokal seperti *Local Area Network* (LAN) dan intranet. Bhardwaj (2007 : 466) lebih lanjut menjelaskan bahwa *private IP address* atau *unregistered IP address* digunakan di dalam jaringan komputer yang bersifat *private*, tidak terkoneksi dengan jaringan *internet*, berada di belakang *proxy server* dan *firewall*, dan terbatas hanya kepada *user* yang berada dalam satu organisasi. *Private IP address* tidak bisa digunakan dalam jaringan publik atau *internet* (Mark Edward Soper, 2004). *Private IP address* tidak mempunyai sifat *globally unique* dan hanya bisa diberikan ke *host* dalam jaringan lokal (Panwar, 2004 : 172).

Tabel 2.2 Private IP Address

Kelas	IP Address	Subnet Mask	Prefix
A	10.0.0.0 – 10.255.255.255	255.0.0.0	10./8
B	172.16.0.0 – 172.31.255.255	255.240.0.0	172.16/16
C	192.168.0.0 – 192.168.255.255	255.255.0.0	192.168/24

(sumber : Sofana, 2010 : 261)

2.2.9. Public IP Address

Public IP address merupakan *IP address* yang digunakan untuk keperluan *internet*. Bhardwaj (2007 : 466) menjelaskan bahwa *public IP address* atau *registered IP address* adalah alamat yang digunakan sebuah jaringan yang dapat diakses dari luar organisasi. Jika sebuah organisasi mempunyai kebutuhan untuk mengkoneksikan jaringannya ke *internet*, maka organisasi tersebut harus memperoleh *public IP address* dari *Internet Service Provider (ISP)*. *Public IP address* mempunyai sifat *globally unique* dan ditetapkan oleh *Internet Corporation for Assigned Names and Numbers (ICANN)*.

2.2.10. Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (ICMP) merupakan protokol yang berada di layer tga yang berfungsi untuk memastikan bahwa host tujuan dalam bisa diakses atau tidak. Ada dua kemungkinan ketika *ICMP request packet* ditolak oleh host tujuan. Kemungkinan pertama adalah bahwa host tujuan dalam keadaan mati atau tidak menyala, sedangkan kemungkinan kedua adalah bahwa *port ICMP* pada host tersebut memang ditutup sehingga tidak bisa diakses oleh *ICMP*. Dalam suatu sistem *connectionless* setiap *gateway* akan melakukan pengiriman, perutean *datagram* yang datang tanpa adanya koordinasi dengan pengirim pertama. Tidak semua sistem berjalan dengan lancar. Kegagalan dapat saja terjadi. misalnya line komunikasi, prosesor atau dikarenakan mesin tujuan tidak sedang aktif, *time-to-live* dari *counter* habis, atau ketika terjadi kemacetan sehingga *gateway* tidak lagi

bisa memproses paket yang datang. Dalam koneksi dengan internet pengirim tidak dapat memberitahukan dan tidak tahu sebab kegagalan suatu koneksi. Untuk mengatasinya diperlukan suatu metode yang memungkinkan gateway melaporkan *error* atau menyediakan informasi mengenai kejadian yang tidak diinginkan sehingga dipakai mekanisme ICMP.

Pesan ICMP merupakan bagian dari datagram IP. Tujuan akhir dari suatu pesan ICMP bukan merupakan program atau user melainkan software internet-nya. Ketika pesan ICMP hadir software ICMP akan menanganinya. ICMP memungkinkan gateway untuk mengirim pesan *error* ke gateway lain atau host. ICMP menyediakan komunikasi antar software protocol Internet. Pada dasarnya terdapat dua macam pesan ICMP : ICMP *Error Message* dan ICMP *Query Message*. ICMP *error message* digunakan pada saat terjadi kesalahan pada jaringan, sedangkan *query message* adalah jenis pesan yang dihasilkan oleh protokol ICMP jika pengirim paket menginginkan informasi tertentu yang berkaitan dengan kondisi jaringan.

Secara teknis ICMP adalah mekanisme *error reporting* untuk gateway sehingga dapat memberitahu sumber mengenai kesalahan yang terjadi. Sedangkan untuk koreksinya diserahkan pada program aplikasi yang ada pada pengirim. Pesan ICMP ini selalu dikirimkan kepada gateway awal. Jika suatu datagram yang melewati beberapa gateway mengalami kegagalan dan kesalahan tujuan di intermediate gatewaynya maka tidak dapat dideteksi gateway mana yang gagal tersebut.

2.2.11. Metode Penelitian

Pada penelitian ini metode penelitian yang digunakan adalah *PPDIOO* (*Prepare, Plan, Design, Implement, Operate and Optimize*) adalah sebuah metode penelitian yang dikembangkan oleh *Cisco System* (*Cisco, 2007*). Metode ini dipilih karena cocok dengan sistem dan pengujian yang akan dilakukan. Metode ini terdiri dari 6 fase yaitu :

1. *Prepare*

Prepare adalah tahap melakukan persiapan terhadap objek yang akan diteliti. Persiapan mencakup mengidentifikasi masalah yang ada diobyek penelitian, solusi-solusi yang akan diambil untuk pemecahan masalah, mempersiapkan buku dan literature yang mendukung penelitian, *browsing* internet terkait dengan jurnal-jurnal yang bisa digunakan sebagai acuan untuk penyelesaian penelitian.

2. *Plan*

Plan adalah tahapan perencanaan terhadap terhadap pelaksanaan penelitian yang mencakup perencanaan bahan penelitian dan alat penelitian. Pada perencanaan alat penelitian, peneliti mempersiapkan perancangan sistem dengan menggunakan *flowchart* dan bahasa pemrograman yang akan digunakan sebagai media untuk membangun sistem.

3. *Design*

Design merupakan tahapan awal pembangunan sistem. Pada tahap ini peneliti berusaha menggambarkan perancangan sistem. Perancangan sistem dibuat sesuai dengan metode yang akan digunakan dalam membangun sistem *bandwidth*

adaptif. pada tahap design ini, peneliti membuat design sistem dengan menggunakan *flowchart* sebagai diagram alur pembangunan sistem. Selain itu, pada tahap ini peneliti juga membuat Rancangan *User Interface* yang menampilkan *layout* sistem yang akan dibangun.

4. *Implement*

Implement adalah tahap membangun sistem yang akan dipakai untuk memecahkan masalah yang ditemui di obyek penelitian. Pada tahap ini, peneliti mengimplementasikan perancangan sistem yang mencakup diagram alur dan dan *layout* sistem kedalam bahasa pemrograman.

5. *Operate*

Operate merupakan tahapan untuk menguji coba sistem bandwidth adaptif yang sudah dirancang dan dibangun apakah sesuai dengan design dan kerangka teori. Pada tahapan ini juga diuji apakah sistem yang dibangun sudah sesuai dengan kebutuhan terhadap permasalahan yang terjadi di obyek penelitian.

6. *Optimize*

Optimize ini adalah tahap terakhir dengan melakukan analisa terhadap sistem sesuai dengan kebutuhan.

BAB 3

CARA PENELITIAN

3.1 Bahan Penelitian

Analisis kebutuhan sistem merupakan proses identifikasi dan evaluasi permasalahan-permasalahan yang ada, sehingga dapat dibangun sebuah sistem yang sesuai dengan yang diharapkan.

Sistem *bandwidth* adaptif pada Jaringan Komputer ini dibuat untuk kebutuhan sebagai berikut :

1. Mampu mengatur alokasi *bandwidth* secara merata ke *Client* dengan memanfaatkan *Internet Control Message Protocol (ICMP)*?
2. Mampu mengatur banyaknya penggunaan batas maksimum *bandwidth internet* secara otomatis pada masing-masing komputer *client*?
3. Mampu melihat banyaknya *traffic data* dalam jaringan?
4. Mampu melakukan *monitoring* komputer *client* dan melakukan pemetaan jaringan bagi komputer *server* dan *client* yang aktif maupun yang tidak aktif?

3.1.1 Analisis Jaringan Komputer Lab Cisco STMIK PROVISI

Lab Cisco mempunyai jaringan komputer dengan topologi star yang mempunyai 1 komputer server (komputer instruktur), 14 komputer client (komputer student) dan 1

switch yang mengkoneksikan semua komputer ke router sehingga bisa terhubung ke internet. STMIK PROVISI mempunyai beberapa jaringan lokal virtual yang terhubung ke 1 server internet. Masing-masing jaringan komputer virtual mendapatkan alokasi sejumlah *bandwidth*. Sistem adaptif *bandwidth* akan dipasang pada server untuk membagi *bandwidth* yang dialokasikan oleh server ke semua komputer dalam jaringan tersebut. Uji coba sistem bandwidth akan dilakukan dengan menggunakan 10 komputer client yang terhubung ke komputer server yang sudah terinstal sistem *bandwidth* adaptif untuk mengetahui *data transfer rate* pada tiap-tiap komputer client. Protokol yang digunakan dalam uji coba tersebut adalah http.

Selain pengujian online internet, pengujian juga dilakukan dengan menggunakan jaringan komputer lokal. Adapun pengujian yang dilakukan adalah pengujian *Performance* dan pengujian *Endurance*.

Pengujian *Performance* dilakukan dengan cara menginstal tools iperf.exe pada komputer client maupun komputer server. iperf merupakan tools yang digunakan untuk mengetahui kinerja sebuah jaringan dengan mengetahui *bandwidth* maksimal dan *data transfer rate* maksimal. Iperf client akan mengirimkan sebuah packet ke server, kemudian server akan merespon packet tersebut dengan mengirimkan *bandwidth* maksimal dan *data transfer rate* maksimal yang dialokasikan ke client tersebut.

Pengujian *Endurance* dilakukan untuk mengetahui ketahanan sistem dengan cara mendownload dengan kecepatan maksimal. Pengujian dilakukan dengan memanfaatkan tools FileZilla yang menggunakan File Transfer Protocol.

3.1.2 Metode Penelitian Lapangan

Pada metode ini, pengumpulan data didapatkan dengan melakukan observasi dan *interview* terhadap dosen, mahasiswa, sebagai berikut:

1. Observasi

Pada tahap observasi ini pengumpulan data dilakukan dengan mengamati konsumsi *bandwidth* dari pemakai internet melalui *bandwidth monitoring*.

2. Wawancara (*Interview*)

Pada tahap wawancara ini, pengumpulan data dilakukan dengan cara mewawancarai secara langsung administrator jaringan, dosen, dan mahasiswa tentang pembagian *bandwidth* dalam jaringan komputer.

3.1.3 Metode Kepustakaan

Metode kepustakaan pada penelitian dilakukan *surfing* atau penjelajahan pada internet sehingga didapatkan beberapa jurnal, artikel dan beberapa *e-book* yang selanjutnya dijadikan acuan pada penelitian ini, serta dilakukan diskusi dengan administrator dan praktisi jaringan yang kompeten di bidangnya dan berbagai masukan dan informasi secara umum mengenai proses analisa *bandwidth* adaptif, ICMP, *Bandwidth Monitoring*.

3.1.4 Analisis Masukan

Setelah melihat akan kebutuhan di atas, maka masukan yang diperlukan untuk memenuhi kebutuhan sistem adalah :

- Konsumsi *bandwidth* baik dosen, karyawan maupun mahasiswa di lingkungan STMIK PROVISI Semarang yang sangat tidak merata.

3.1.5 Analisis Keluaran

Tahapan ini berfungsi untuk mengetahui keluaran apa saja yang akan dihasilkan dari sistem yang dibangun. Adapun spesifikasi keluaran dalam bentuk :

- Sistem informasi kapasitas *bandwidth* yang diterima dari ISP dan distribusi *bandwidth* tersebut ke semua komputer yang aktif.
- Data-data pengguna internet dalam satu *workgroup*, yang mencakup *IP address*, *computer name*, *MAC address*, alokasi *bandwidth* yang diterima, jenis paket data yang diterima, jenis protokol aplikasi dan jenis protokol transport yang melewati jaringan komputer yang di *capture* oleh sistem *bandwidth* adaptif.

3.1.6 Analisis Profile Pengelola Sistem.

Adapun profile dari pengelola sistem ini adalah:

1. Administrator

Sistem *Bandwidth* adaptif ini digunakan oleh administrator untuk memonitor komputer yang aktif dalam satu jaringan dan kemudian mendistribusikan *bandwidth* yang diterima dari *Internet Service Provider (ISP)* ke semua komputer yang aktif.

2. Operator

Operator adalah staff yang diberi wewenang/hak oleh administrator untuk menggantikan tugas dan tanggung jawab administrator jika diperlukan.

3.1.7 Syarat Pengetahuan Pengelola Sistem

Sistem *Adaptive Bandwidth* mendeteksi kapasitas *bandwidth* yang diterima. Sistem ini juga memonitor semua *client* yang aktif dan kemudian membagi *bandwidth* secara merata. Kekurangan *bandwidth* yang diterima *client* bisa diakibatkan dua hal yaitu: dari *Internet Service Provider (ISP)* yang mengalami *congestion* atau memang jumlah *client* yang aktif sangat banyak sehingga kapasitas *bandwidth* akan terbagi ke banyak *client* dan *throughput* yang diterima oleh *end user* menjadi sedikit juga. Untuk itu administrator dan operator disyaratkan mempunyai pengetahuan yang memadai mengenai jaringan komputer, setidaknya memiliki kemampuan :

A. Administrator

1. Memiliki pengetahuan jaringan komputer.
2. Memiliki pengetahuan tentang keamanan jaringan komputer dan karakteristik penyusup pada jaringan komputer.
3. Memiliki kemampuan tentang perhitungan *bandwidth* dan *throughput*.
4. Memiliki kemampuan untuk melakukan *troubleshooting* pada jaringan sesuai dengan kaidah pemecahan masalah pada jaringan komputer.

B. Operator

1. Memiliki pengetahuan dasar-dasar jaringan komputer, seperti IP Address, MAC address, Subnet Mask.
2. Memiliki pengetahuan tentang enkapsulasi pada data.
3. Memiliki pengetahuan tentang keamanan jaringan komputer dan protokol-protokol pada jaringan komputer.
4. Memiliki kemampuan perhitungan *bandwidth* dan throughput.

3.2 Alat Penelitian

Kebutuhan Perangkat Keras

- Prosesor dengan kecepatan 1.6 GHz.
- RAM 512 MB.
- Kapasitas harddisk 20 GB.
- Keyboard + Mouse.
- *Network Interface Card (NIC)*.
- *UTP Cable Cat 5e*

Kebutuhan Perangkat Lunak

Perangkat lunak yang digunakan untuk implementasi aplikasi antara lain:

- *Windows XP Operating System Starter Pack 2.*
- *Framework .Net* digunakan sebagai *tools* supaya aplikasi dapat berjalan dengan baik.
- *Microsoft Visual Studio 2005.*

3.3 Jalan Penelitian

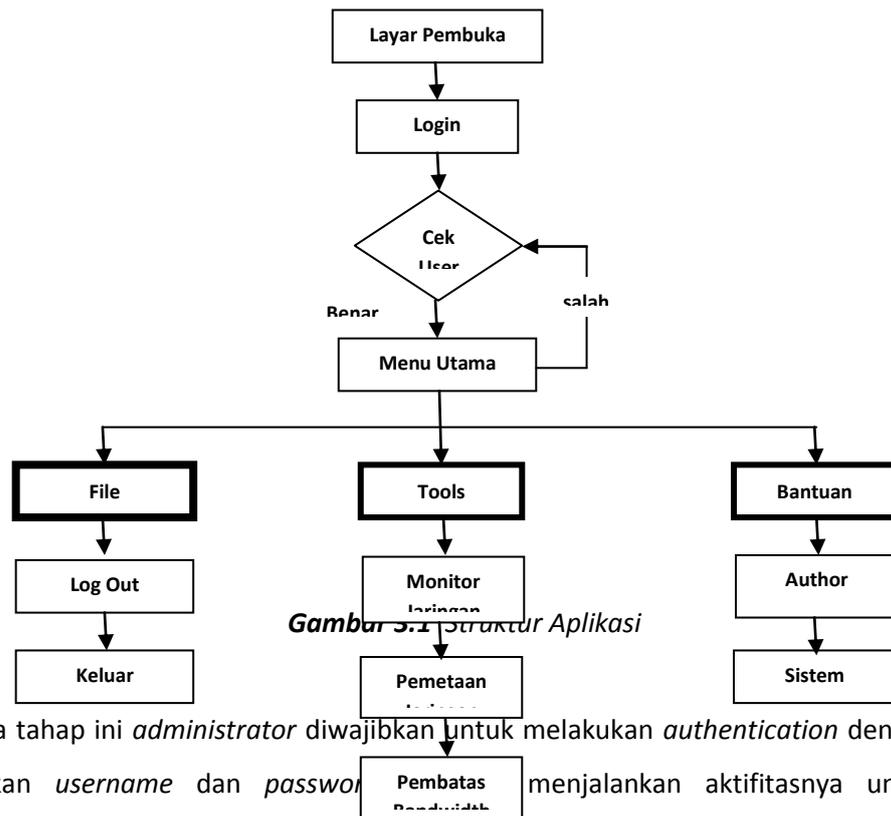
Langkah-langkah yang diambil pada pelaksanaan meliputi perancangan perangkat lunak sebagai berikut:

3.3.1 Flowchart dan Struktur Sistem

Flowchart merupakan gambar atau bagan yang memperlihatkan urutan dan hubungan antar proses beserta instruksinya.

A. Struktur Sistem *Bandwidth* Adaptif

Struktur Sistem *Bandwidth* Adaptif pada Gambar 3.1 menjelaskan tentang aktifitas pertama yang dilakukan administrator.



Gambar 3.1 Struktur Aplikasi

Pada tahap ini *administrator* diwajibkan untuk melakukan *authentication* dengan memasukkan *username* dan *password* menjalankan aktifitasnya untuk menganalisa dan memonitor *bandwidth* yang diterima oleh *end user*. Setelah divalidasi oleh aplikasi, program akan memunculkan beberapa menu pilihan yang akan dianalisa oleh administrator yaitu Monitoring Jaringan, Pemetaan Jaringan, Pembatas Jaringan dan ping tools. Menu-menu tersebut yang akan dijadikan acuan untuk kemudian dianalisa sebagai acuan untuk memonitor banyaknya *bandwidth* yang akan didisbusikan ke semua *end user*.

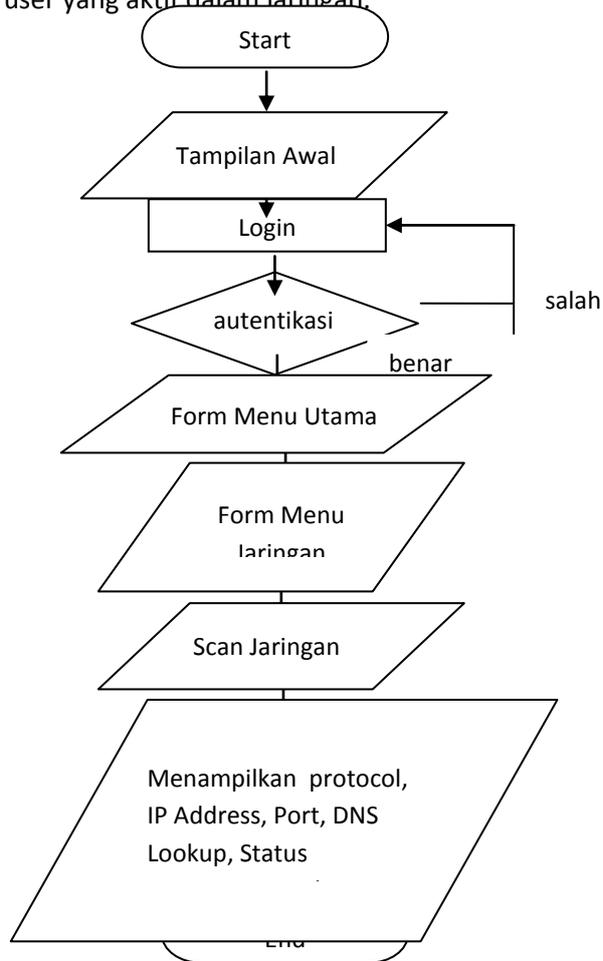
B. Flowchart Monitoring Jaringan

Flowchart Form *Monitor Jaringan* pada Gambar 3.2 menunjukkan bahwa *authentication* sudah dipenuhi sehingga sistem menampilkan menu utama dari program

ini. Pada menu utama menampilkan beberapa menu, salah satunya adalah menu Monitoring Jaringan.

Menu ini bertugas untuk memonitor data yang sedang dikirim dan diterima oleh semua *host* yang aktif dalam jaringan. Pada form ini sistem akan melakukan *scanning* pada jaringan untuk menampilkan data-data protokol transport, IP Lokal, IP Tujuan, Port Lokal, Port Tujuan, DNS Lookup dan Status dalam komunikasi data.

Hasil *scanning* ini merupakan akumulasi dari semua *unit packet* yang masuk dalam sistem yang kemudian akan diproses dalam form pembagi *bandwidth* untuk didistribusikan ke semua user yang aktif dalam jaringan.



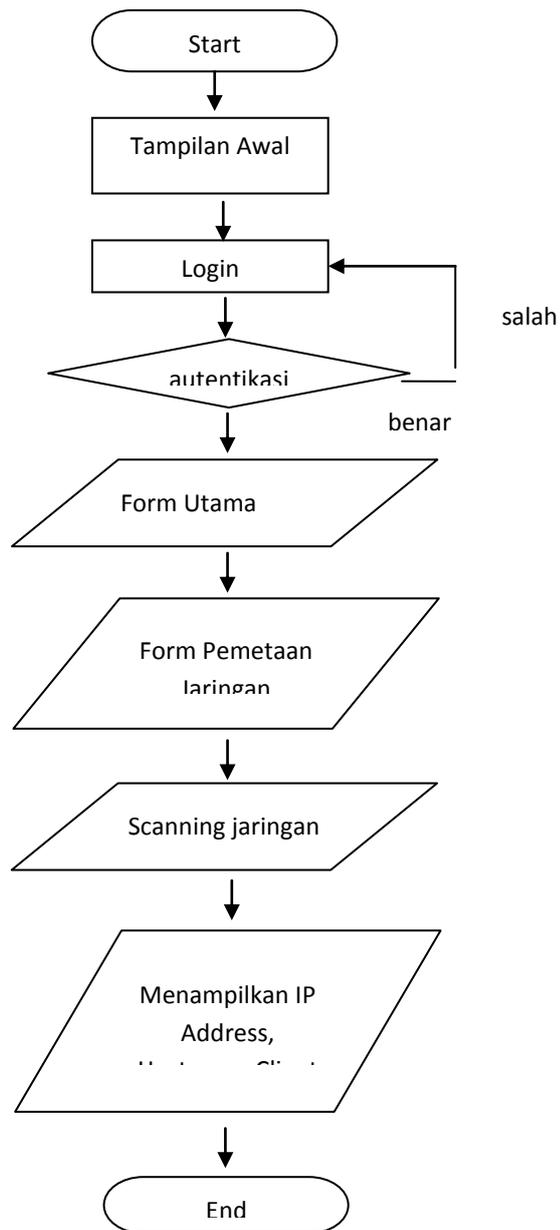
Gambar 3.2 Flowchart Menu Monitoring Jaringan

C. Flowchart Pemetaan Jaringan

Flowchart Pemetaan Jaringan pada gambar 3.3 menunjukkan bahwa administrator menggunakan menu yang kedua yaitu menu Pemetaan Jaringan.

Pada menu tersebut aplikasi akan menampilkan *MDI child* dari form menu utama yaitu form Pemetaan Jaringan. Pada form Pemetaan Jaringan akan melakukan scanning jaringan dengan cara mengirimkan *ICMP Packet Request* kesemua host, bagi host yang sedang aktif akan mengirimkan *ICMP reply packet* ke server.

Semua host yang mengirimkan *ICMP reply* ke server kemudian akan ditampilkan pada form Pemetaan Jaringan yang akan dijadikan acuan untuk menghitung jumlah *host* yang aktif. *Bandwidth* yang diterima oleh server dari *Internet Service Provider* kemudian akan dibagi sesuai dengan jumlah *host* yang aktif dan kemudian didistribusikan ke *host* yang aktif tersebut dalam jaringan.

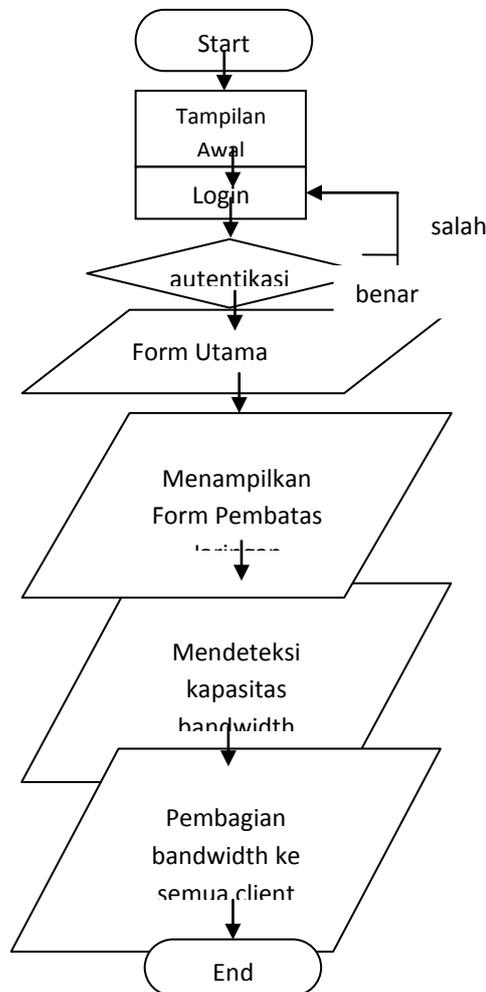


Gambar 3.3 Flowchart Menu Pemetaan Jaringan

D. Flowchart Pembatas Bandwidth

Flowchart Form Pembatas Bandwidth pada Gambar 3.4 menunjukkan bahwa dalam menu utama terdapat menu Pembatas Jaringan. Pada menu tersebut aplikasi akan menampilkan *MDI child* dari form menu utama yaitu form Pembatas *Bandwidth*.

Pada form ini sistem akan mendeteksi kapasitas *bandwidth* yang diterima dari *Internet Service Provider*. Kapasitas *bandwidth* yang diterima menunjukkan jumlah maksimal data yang bisa dikirimkan dari internet ke jaringan lokal.



Gambar 3.4 Flowchart Menu Pembatas Bandwidth

Kapasitas *bandwidth* yang tayangkan pada menu ini selalu akan berubah-ubah jaringan. Perubahan kapasitas *bandwidth* yang tersedia dipengaruhi oleh beberapa faktor diantaranya adalah faktor *congestion*, serangan *denial of service*, *data traffic* dalam jaringan, penurunan kapasitas *bandwidth* dari *Internet Service Provider* (ISP), dan kemampuan prosesor dalam memproses trafik data dalam jaringan. Dari kapasitas *bandwidth* yang diterima oleh *server* tersebut kemudian akan didistribusikan ke semua

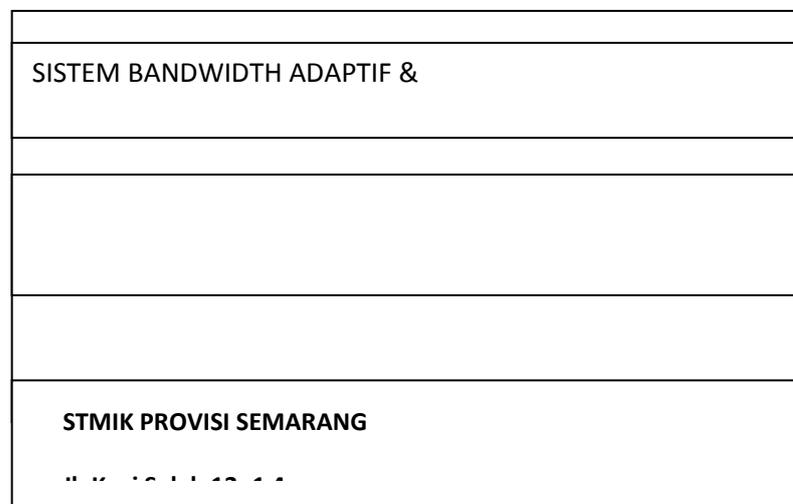
host yang aktif dalam jaringan. Pembagian kapasitas *bandwidth* ditentukan oleh sistem dengan pembagian sama rata.

3.3.1.1 Rancangan *User Interface*

Tampilan sistem ini dibuat berbentuk *desktop* yang dibagi menjadi bagian judul yang terletak pada bagian atas, bagian menu bar yang terletak di bawah bagian judul untuk menempatkan menu *pull-down*, bagian untuk menempatkan tombol-tombol menu, bagian *output* untuk menampilkan hasil kapasitas *bandwidth* yang diterima, kapasitas *host* yang aktif, protokol yang digunakan dalam lalu lintas data. Berikut ini adalah tampilan *user interface* sistem yang dibuat:

a. *Form Tampilan Awal*

Perancangan tampilan *Form ini* merupakan tampilan awal saat aplikasi dijalankan, adapun tampilan awal dirancang seperti pada Gambar 3.5.



Gambar 3.5 Perancangan Layar Pembuka

b. Form Login

Pada form ini ditampilkan *username* dan *password* sebagai authentication untuk menggunakan sistem ini. Pada form ini terdapat dua data yang harus dientrikan:

1. *Username*:

Username merupakan salah satu syarat authentication untuk dalam masuk dalam sistem ini. *Username* merupakan nama pengguna yang telah ditentukan dalam sistem ini.

2. *Password*:

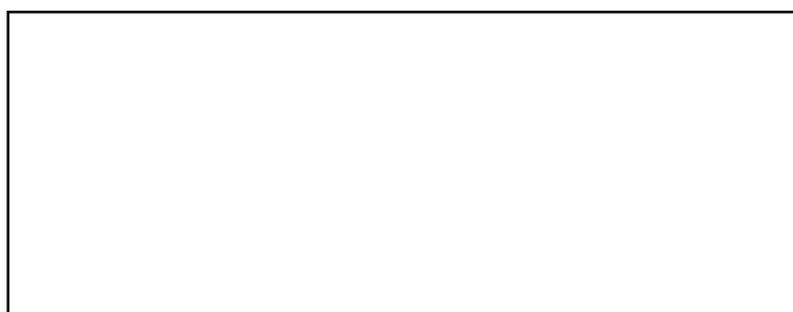
Password merupakan kata kunci yang harus dimasukkan untuk dapat mengakses sistem ini. *Password* kuat akan membuat orang yang tidak berhak sulit untuk membuka mengakses sistem.

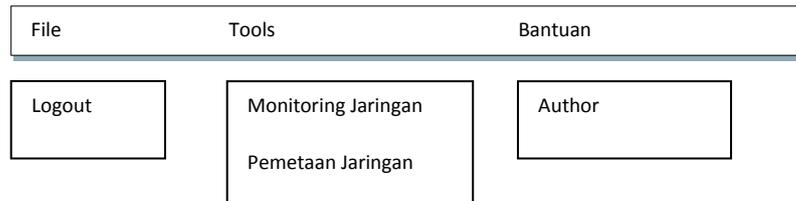
The image shows a login form with a title bar 'Akses Masuk'. Below the title bar, there are two rows of input fields. The first row has a label 'Username' followed by a text input box. The second row has a label 'Password' followed by a text input box. At the bottom of the form, there are two buttons: 'Masuk' and 'Keluar'.

Gambar 3.6 Perancangan Form Login

c. Form Menu Utama

Form Menu Utama akan ditampilkan setelah *Form Layar Pembuka* dan *Form Layar Login*, yaitu setelah *username* dan *password* dimasukkan. Form ini berbentuk *Multiple document Interface* (MDI). Penampilan Form menu utama di dirancang sebagai berikut:

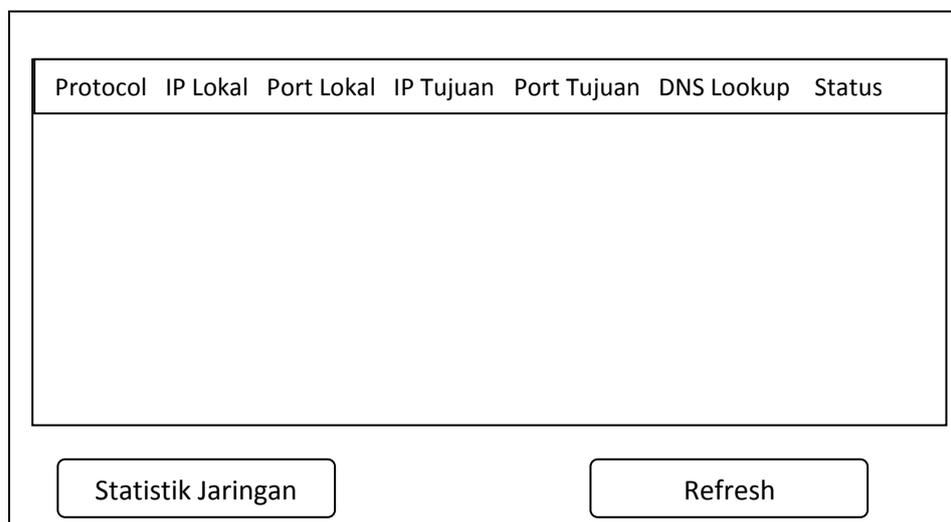




Gambar 3.7 Perancangan *Form* Menu Utama

d. Form Monitor Jaringan

Pada form ini akan ditampilkan *IP address* dan *port* dari semua *host* yang aktif dalam jaringan. *Form* Monitoring Jaringan akan menscan trafik data yang sedang terjadi di jaringan komputer yang melibatkan semua *host* yang aktif. Pada *form* ini juga akan ditampilkan semua protokol yang digunakan selama melakukan komunikasi data. Dalam form ini terdapat tombol *refresh* yang berfungsi untuk mengupdate proses komunikasi data yang sedang terjadi dalam jaringan komputer tersebut. Perancangan Form Monitoring Jaringan ditunjukkan pada Gambar 3.8 sedangkan Form Statistika Jaringan ditunjukkan pada Gambar 3.9.



Gambar 3.8 Perancangan Form Monitor Jaringan

The image shows a wireframe for a network monitoring form. At the top, there are four tabs: "Transmission Control Protocol", "User Datagram Protocol", "IP Global", and "Internet Control Message Protocol". Below the tabs is a table with two columns: "Parameter" and "Value". The table is currently empty. At the bottom of the form, there are two buttons: "Refresh" and "Tutup" (Close).

Parameter	Value
-----------	-------

Gambar 3.9 Perancangan Form Statistika Jaringan

e. Form Pemetaan Jaringan

Form Pemetaan Jaringan merupakan *form* yang digunakan untuk menampilkan *IP address* dari semua komputer yang aktif dalam jaringan. Dari jumlah komputer yang sedang aktif inilah, *bandwidth* yang diterima dari *Internet Service Provider* dibagi dan didistribusikan kesemua komputer yang aktif yang ditampilkan dalam form Pemetaan Jaringan ini. *Form Pemetaan Jaringan* dirancang seperti pada Gambar 3.10.

The diagram shows a rectangular form with a double-line border. At the top, there is a thin horizontal bar. Below it is a section labeled "File". Underneath "File" is a section labeled "Pemetaan Jaringan", which contains a large, empty rectangular box for data entry.

Gambar 3.10 Perancangan Form Pemetaan Jaringan

f. **Form Pembatas Jaringan**

Form Pembatas Jaringan dirancang untuk menampilkan perolehan *bandwidth* dan pembagian *bandwidth* pada *end user*. Pada *form* ini terdapat beberapa *textbox* yaitu kecepatan *bandwidth* yang diterima dari *Internet Service Provider* (ISP) dan alokasi *bandwidth* pada masing-masing komputer yang sedang aktif dalam jaringan. Pada *form* ini juga ditampilkan *interface* jaringan yang sedang aktif dalam jaringan. *Interface* yang mungkin di-capture oleh *form* ini adalah interface ethernet dan *interface wireless* yang sedang aktif dalam jaringan. *Form Pembatas Jaringan* dirancang seperti pada Gambar 3.11.

The diagram illustrates the layout of the 'Form Pembatas Jaringan'. It is enclosed in a rectangular border and divided into several sections:

- Daftar Komputer Aktif:** A large empty rectangular box on the left side, intended for displaying active computers.
- Input Fields:** A central column of four stacked input boxes with corresponding labels:
 - Internet Service Provider
 - Kapasitas Bandwidth
 - Jumlah Komputer Aktif
 - Alokasi Bandwidth Host
- Interface Jaringan:** A large empty rectangular box on the right side, intended for displaying active network interfaces.
- Buttons:** Two buttons are located at the bottom of the form:
 - 'Refresh' button on the left.
 - 'Selesai' button on the right.

Gambar 3.11 Perancangan Form Pembatas Jaringan

3.4 Skenario Pengujian Program

Pengujian program dilaksanakan di laboratorium Cisco STMIK PROVISI dengan memanfaatkan jaringan komputer yang sudah ada. Skenario program dilaksanakan pada

sisi *server* yang bertindak sebagai *router gateway* dan sisi *client* yang menerima distribusi *bandwidth* dari *server*.

1. *Server*

Merupakan komputer yang bertindak sebagai *router gateway* yang terkoneksi langsung dengan *Internet Service Provider*. *Bandwidth* yang diterima oleh *server* kemudian akan dialokasikan oleh sistem *bandwidth* adaptif sehingga bisa diterima oleh semua *client* dalam satu *workgroup* secara merata sesuai dengan jumlah *client* yang aktif.

2. *Client*

Merupakan komputer yang menerima *bandwidth* dari *server*. Jumlah *client* dalam jaringan komputer sangat bervariasi tergantung dengan jumlah user yang menggunakan koneksi *internet*. *Client* yang terhubung ke jaringan akan diberikan nama *workgroup* yang sama sebagai *token* bahwa komputer tersebut berada dalam satu *workgroup*. Alokasi *bandwidth* akan dieksekusi berdasarkan pada nama *workgroup* yang sama. Komputer *client* yang mempunyai nama *workgroup* yang berbeda tidak akan menerima alokasi *bandwidth* dari *server*. Pada skenario ini juga dicoba menggunakan beberapa *software* yang akan menjadi alat bantu untuk menghitung kapasitas *bandwidth* yang diterima oleh *client* seperti *Internet Download Manager* dan beberapa web yang akan diakses untuk mengetahui jumlah *bandwidth* yang diterima.

3.5 Kesulitan-kesulitan

Kesulitan-kesulitan dalam penelitian yang ditemui adalah:

1. Mencari solusi atas permasalahan yang terjadi pada obyek penelitian dimana terjadi distribusi *bandwidth* yang tidak merata disemua *client*.
2. Penerapan teori kedalam *coding* yang harus menyesuaikan dengan kerangka kerja (*frame work*) bahasa pemrograman yang digunakan.

DAFTAR PUSTAKA

- Afdhal & Gani, A.T., 2005, *Pemantauan Workstation Pada Jaringan komputer Lokal Dengan Memanfaatkan Layanan SNMP*, Rekayasa ElektriKa.
- Ariyus, Doni, 2007, *Intrusion Detection System*, Yogyakarta: Penerbit ANDI.**
- Kurinawan, Wiharsono, 2007, *Computer Starter Guide: Jaringan Komputer*, Yogyakarta: Penerbit ANDI.
- Nagaraja, Chittal, Kumar, 2007, *Study of Network Performance Monitoring Tools-SNMP*, International Journal of Computer Science and Network Security.
- Nugroho, Adi, 2007, *Analisis dan Perancangan Sistem Informasi Berorientasi Obyek*, Bandung: Informatika.
- Nyirenda, Mwanza, Aruoture, 2002, *Network Performance Monitoring*, <http://www.oppapers.com/essays/Network-Performance-Monitoring/>, diakses tanggal 3 November 2009.
- Pressman, Roger, 2002, *Rekayasa Perangkat Lunak: Pendekatan Praktisi (Buku Satu)*, Yogyakarta: Penerbit ANDI dan McGraw-Hill Book Co.
- Pressman, Roger, 2005, *Software Engineering: A Practitioner's Approach, Sixth Edition*, New York: The McGraw-Hill Companies, Inc.