PROTOKOL TCP/IP SEBAGAI SARANA DALAM PROSES TRANSFER DATA

Mahmud Yunus [1] M. As'ad [2]

ABSTACT

The study entitled Protocol TCP / IP as a means to transfer this data, carried out in laboratory STMIK PPKIA Pradnya Paramita Malang in order to find out how the working process of the protocol TCP / IP and obtain a clear picture of how the protocol TCP / IP plays a role in communication within the user's computer internet. This research is the development presented in descriptive form, which is analyzing the data transfer process is one of them by using the protocol TCP / IP. The results could determine the level of error that occurred while sending and receiving data, and can be used as a reference untu networking development.

***Keywords**:Protocol, Protocol TCP/IP, Transfer Data.*

PENDAHULUAN

Salah satu hal yang sangat penting yang perlu diketahui dalam rangka memasuki dan memanfaatkan globalisasi ini, adalah pengetahuan teknis yang cukup dalam hal komunikasi data. Untuk dapat memanfaatkan sumber-sumber data yang diperlukan suatu sistem komputer yang dapat menghubungkan pemakai (*user*) dengan sumber data tersebut.

Sistem jaringan komunikasi data yang sangat populer dan tersebar di seluruh dunia adalah jaringan internet. Jaringan ini menghubungkan antara satu host komputer dengan komputer lainnya yang tersebar di seluruh dunia dengan menggunakan protokol IP atau disebut juga dengan internet protokol.

Dewasa ini sudah semakin banyak pemakai komputer yang menggunakan internet, tetapi masih banyak pemakai yang belum mengetahui secara jelas tentang bangaimana sebenarnya komputer-komputer tersebut dapat salaing berhubungan dan bertukar informasi meskipun dalam tempat yang berbeda. Oleh karena itu peneliti mengambil pokok permasalahan tentang salah satu macam internet protokol, yaitui protokol TCP/IP untuk dipakai sebagai bahan penelitian ini.

KAJIAN TEORI

1. Jaringan Komputer

Pada awalnya komputer dihubungkan dengan komputer lain dengan tujuan pertukaran data secara sederhana. Teknologi yang ada yaitu *Serial Interface* (RS232) dapat digunakan untuk

[1] Dosen STMIK PPKIA Pradnya Paramita Malang
[2] Dosen STMIK PPKIA Pradnya Paramita Malang

menghubungkan dua komputer secara langsung (*direct*) atau melalui modem dan untuk selanjutnya dihubungkan dengan fasilitas seperti telepon atau lainnya. Bentuk hubungan ini disebut dengan *Wide Area Network* (WAN).

Munculnya teknologi *Local Area Network* (LAN) yang menggunakan ethernet atau lainnya pada tahun 1970-an memungkinkan komputer untuk saling berhubungan dengan kecepatan 10.000bps (10 Mbps) memberikan inovasi baru. Berbeda dengan WAN, umumnya komputer LAN terletak satu dengan yang lainnya dalam radius yang tidak terlalu jauh (dalam satu gedung atau kompleks).

Utilities jaringan ini tidak terbatas pada pertukaran atau transfer data saja, tapi dapat juga memberikan layanan-layanan lain yang spesifik. Ide ini melahirkan konsep *client server* dimana jaringan dapat terdiri dari sebuah komputer yang berfungsi sebagai *server*, sebagai *client* atau sekaligus sebagai *server* dan *client*. Dengan demikian *server* adalah *host* yang memberikan layanan yang spesifik, sedangkan client adalah komputer/*workstation* yang meminta layanan tersebut.

a. Token Ring

Komputer dihubungkan satu dengan lainnya dengan membentuk lingkarang (*ring*). Data berjalan satu arah mengelilingi lingkaran sehingga sampai ke simpul (*node*) yang dituju. Bila salah satu peserta jaringan mengalami kerusakan, maka hubungan dilanjutkan ke komputer berikut (*short circuit*) dengan demikian komunikasi tetap berjalan.

b. *Star Network*

Dalam jaringan ini komputer-komputer dihubungkan dengan satu kendali pusat (*central device control*) atau disebut juga *hub. Hub* menerima paket data dari komputer dan meneruskannya ke tempat tujuan. Keuntungan model jaringan ini adalah jarak yang diperlukan untuk mengirim paket dari satu simpul ke simpul yang lain sangat cepat.

c. *Bus Network*

Peserta jaringan dihubungkan dengan satu kabel (disebut = *bus*). Tranmisi data dilakukan oleh satu host di jaringan dan hanya dapat dilakukan bila bus sedang tidak digunakan oleh host yang lain. Bila terjadi tabrakan tranmisi antara dua host atau lebih, maka tranmisi akan diulang.

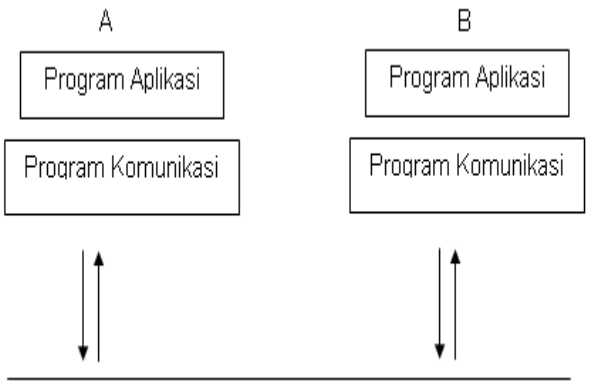
2. Protokol Komunikasi

Bila dua kumputer berkomunikasi satu dengan yang lainnya maka dibutuhkan satu media fisik yang menyampaikan data (*message*) dari satu komputer ke komputer yang lain. Dalam penyimpanan data oleh program aplikasi, maka harus ada program rutin yang bertugas

[1] Dosen STMIK PPKIA Pradnya Paramita Malang
[2] Dosen STMIK PPKIA Pradnya Paramita Malang

mengirimkan dan menerima data ke dan dari media komunikasi.

Gambar 1 di bawah ini menggambarkan pengiriman dan penerimaan data ke dan dari media komunikasi.



Gambar 1 Pengiriman dan Penerimaan Data

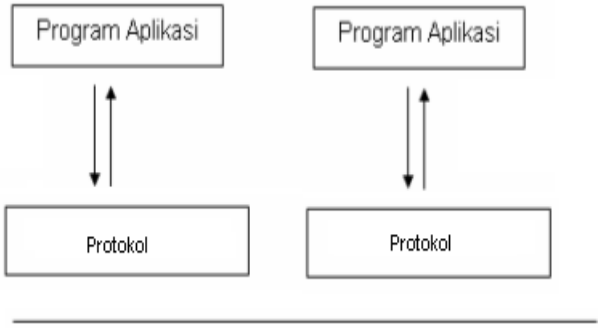
Komunikasi antar program ini ternyata memerlukan suatu aturan, yaitu tatacara bagaimana mereka dapat saling mengenal dan melakukan data transfer tanpa *error* . Untuk itu diperlukan tata cara sebagai berikut :

1. Menyatakan akan mengadakan transfer data
2. Menjawab bahwa komputer siap untuk transfer data.
3. Menyatakan bahwa data dikirim sebanyak sekian karakter (*bytes*)
4. Menjawab bahwa data telah dikirim
5. Menjawab bahwa data yang dikirm diterima dengan kondisi *error,* sehingga perlu diulang
6. Menyatakan bahwa transfer data selesai.

Kesemua ini adalah aturan yang kemudian disebut sebagai protokol. Data transfer hanya dapat dilakukan oleh komputer, bila mereka mempunyai protokol yang sama.

Berdasarkan buku *Practical Internet Working With* TCP/IP *and* UNIX , 1993 ada beberapa hal yang dapat diselesaikan dengan menggunakan bantuan protokol, antara lain :

1. Data Delivery : Mengirimkan paket sampai tujuan (*destination*)
2. Error Detection : Mendeteksi kesalahan tranmisi melalui CRC, Checksum Nomor Urut Paket, AC Knowledge, Timer dan lainnya.
3. Error Corection : Mengoreksi kesalahan tranmisi secara otomatis dengan menggunakan algoritma tertentu, atau meminta pengulangan transmisi.



Gambar 2 Transfer Data Menggunakan Protokol yang sama

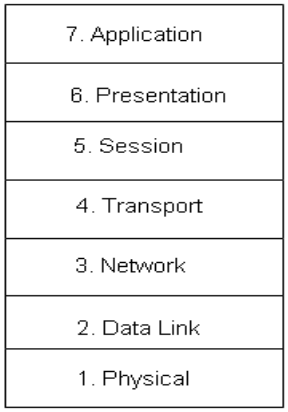
4. Protokol OSI (*Open System Inter Connection*)

International Organization for Standardization (ISO) telah mengembangkan sebuah model dari arsitektur jaringan yang diberi

[1] Dosen STMIK PPKIA Pradnya Paramita Malang
[2] Dosen STMIK PPKIA Pradnya Paramita Malang

nama *Open System Inter Connection* (OSI). Tujuan dari pembuatan model ini adalah untuk mempromosikan interkonsi antar jaringan yang beragam.

Prinsip dari model OSI adalah lapisan (*layer*) yang setiap lapisan mempunyai fungsi yang spesifik. OSI memberikan tujuh lapisan sebagai berikut :



Gambar 3 Tujuh Lapisan / Tingkatan OSI

5. Protocol TCP/IP

TCP/IP lahir dari sebuah proyek yang dibiayai oleh *Defense Advanced Reasearch Project Agency* (DARPA) pada tahun 1969, jauh sebelum model OSI dipublikasikan. TCP/IP mulai popular pada pengembangan di Universitas Barkely Amerika Serikat dan implementasinya dalam sistem berbasis UNIX (Barkeley Version)

TCP/IP (*Tranmission Control Protocol/Internet Protocol*) memungkinkan hubungan virtual antar komputer, dimana dua komputer atau lebih akan dapat saling berhubungan untuk pertukaran data serta layanan aplikasi jaringan lainnya.

Tujuan daripada desain TCP/IP adalah sebagai berikut :

1. Standart protokol yang open. Artinya spesifikasi dapat diperoleh dengan bebas dan dikembangkan sesuai dengan hardware yang dimiliki. Dengan demikian TCP/IP dapat diimplementasikan pada platform hardware yang beragam.

2. Tidak tergantung pada jaringan fisik hardware. TCP/IP dapat diintegrasikan pada jaringan fisik yang bermacam-macam melalui ethernet, token ring, dial up (telepon) RS232 dan media tramsmisi lainnya.

3. Skema address yang luas. Skema adress internet memungkinkan komputer mempunyai identitas tunggal (IP-address), sehingga walaupun mempunyai jangkauan international (wordwide), komputer manapun dapat dicapai dengan mudah karena mempunyai identitas yang jelas.

4. Standar aplikasi. Utilitas standar yang akan memudahkan pemakaiannya dalam melakukan file transfer, *remote login* dan *remote execution*.

[1] Dosen STMIK PPKIA Pradnya Paramita Malang
[2] Dosen STMIK PPKIA Pradnya Paramita Malang

6. *Network Interface Layer*

Layer ini bertanggung jawab mengirim data dan menerima data dari media fisik. Beberapa contoh *Network Interface Layer* adalah :

a. *Ethernet*

Jika kita mengenal *Local Area Network* (LAN), maka kita mengenal *Interface Ethernet.* Model *Interface Ethernet* ditemukan di Xerox *Palo Alto Research Center* (PARC) di tahun 1970-an oleh Dr. Robert M. Metcalfe. Ethernet pertama berjalan dengan kecepatan 3 Mbps dan dikenal sebagai *Ethernet Eksperimental.*

Interface ini merupakan sebuah card yang terhubung ke card yang lain melalui ethernet hub dan kabel UTP atau hanya menggunakan sebuah kabel BNC yang diterminasi di ujungnya.

Dasar pemikiran dirancangnya ethernet ialah "berbagi kabel". Lebih dari dua komputer dapat menggunakan satu kabel untuk berkomunikasi. Karena hanya digunakan satu kabel saja, maka proses pemancaran data harus dilakukan bergantian. Mirip ketika terjadi pembicaraan di forum atau rapat. Jika seseorang sedang berbicara, maka orang lain seharusnya diam dan mendengarkan. Jika pada saat bersamaan terdapat dua orang yang berbicara, pendengar akan merasa terganggu.

Sebelum satu card ethernet memancarkan datanya pada kabel, dia harus mendeteksi terlebih dahulu ada tidaknya card lain yang sedang memancar. Jika tidak ada maka dia akan memancar. Jika ada maka card ethernet akan menunggu sampai kabel dalam keadaan kosong. Jika pada saat bersamaan dua card memancarkan data maka terjadilah *collison* / tabrakan (hal ini dideteksi oleh card yang bersangkutan dengan memeriksa tegangan kabel, jika tegangan ini melampaui batas tertentu, maka terjadi *collison*). Jika *collison* terjadi maka masing-masing card berhenti memancar dan menunggu lagi dengan selang waktu yang acak untuk mencoba memancar kembali. Karena selang waktu pancar masing-masing card yang acak ini, maka kemungkinan *collison* lebih lanjut menjadi lebih kecil.

Karena dalam satu kabel terdapat banyak card ethernet, maka kita harus mempunyai suatu metode untuk mengenali dan membedakan masing-masing card ethernet tersebut. Untuk itu, pada setiap card ethernet telah tertera kode khusus sepanjang 48 bit yang dikenal sebagai *ethernet address.*

b. SLIP (*Serial Line Interface Protocol*)

Selain ethernet interface jaringan yang sangat banyak dipakai ialah modem telepon, yang dihubungkan ke komputer melalui media port. Salah satunya adalah SLIP (*Serial Line Interface Protocol*) ialah teknik enkapsulasi datagram yang paling sederhana di internet. Datagram IP yang diterima dienkapsulasi dengan menambah karakter END (0xC0) pada awal dan akhir frame .

[1] Dosen STMIK PPKIA Pradnya Paramita Malang
[2] Dosen STMIK PPKIA Pradnya Paramita Malang

Jika pada datagram terdapat karakter 0xC0, karakter ini diterjemahkan sebagai karakter SIP ESC, yaitu 0xDB 0xDC. Jika pada datagram sudah terdapat karakter 0xDB karakter ini diubah menjadi 0xDB 0xDD.

c. PPP (*Point to Point Protocol*)

PPP terdiri atas beberapa protokol mini sebagai berikut :

1. LCP (*Link Control Protocol*) LCP ini berfungsi membentuk dan memelihara link.
2. *Authentication Protocol.* Protokol ini digunakan untuk memerikasa boleh tidaknya user menggunakan link ini. Ada dua jenis autentikasi yang umum digunakan yaitu *Password Authentication Protocol* (PAP) dan *Challenge Handshake Authentication Protocol* (CHAP)
3. *Network Control Protocol* (NCP), berfungsi mengkoordinasikan operasi bermacam-macam protokol jaringan melalui link PPP ini. Beberapa hal yang dilakukan oleh protokol ini adalah menegosiasikan jenis protokol kompresi yang akan dipakai serta menanyakan IP address mitranya.

Internet Layer

a. IP (*Internet Protocol*)

Lapisan ini mengorganisasikan pengiriman data ke host yang dituju melalui network address dan disebut juga sebagai *Internet Protocol* (IP). Protokol ini mensyaratkan bahwa setiap host (simpul) mempunyai address tunggal (*unique*). Address ini adalah identitas host sebagai IP-address. Network Layer bertanggung jawab untuk menciptakan hubungan komunikasi (*establishment*), kelancaran sehingga selama komunikasi dan mengakhiri komunikasi (*termination*). Internet protokol mengirim paket secara *unreliable* atau disebut juga sebagai *connectionless. Unreliable* artinya internet protokol tidak memberikan jaminan atas keberhasilan pengiriman paket tersebut. Protokol ini menyerahkan tanggung jawab tersebut kepada lapisan/layer diatasnya. Setiap pengiriman IP-data paket tidak diperlukan AC knowledge atau jawaban dari si penerima, apakah paket tersebut telah diterima dengan baik atau tidak. Disebut *connectionless* karena protokol ini memerlukan inisialisasi hubungan, artinya IP mengirimkan paket tanpa lebih dulu memberi tahu partner yang dituju (analogi dengan POS). *Datagram Delivery Service* berarti setiap paket data yang dikirim adalah independen terhadap paket data yang lain. Akibatnya jalur yang ditempuh masing-masing data IP ke tujuannya bisa jadi berbeda satu dengan lainnya. Karena jalur yang ditempuh berbeda, kedatangan paketpun bisa jadi tidak beraturan.

[1] Dosen STMIK PPKIA Pradnya Paramita Malang
[2] Dosen STMIK PPKIA Pradnya Paramita Malang

Version	Header Length	Typoe of Service	Total Length of Datagram
Identification		Flags	Fragment Offset
Time to Live	Protocol	Header Checksum	
Source IP Address			
Destination IP Address			
Option : Strict Source Routing, Loose Source Routing			
DATA			

Gambar 4 Format Datagram IP

Pada gambar 4 diberikan format datagram IP. Setiap paket IP membawa data yang terdiri atas :

- *Version,* berisi versi dari protokol IP yang dipakai. Pada saat ini versi IP yang dipakai adalah IP versi 4.
- *Header Length,* berisi panjang dari header paket IP dalam hitungan 32 bit word
- *Typoe of Service,* berisi kualitas service yang dapat mempengaruhi cara penanganan IP
- *Total Length of Datagram,* panjang IP datagram total dalam ukuran byte.
- *Identification, Flags,* dan *Fragment Offset.* Berisi beberapa data yang berhubungan dengan fragmentasi paket. Paket yang dilewatkan memlalui berbagai jenis jalur akan mengalami fragmentasi (dipecah menjadi beberapa paket yang lebih kecil) sesuai dengan besar data maksimal yang bisa ditramisikan melaluki jalur tersebut.
- *Time to Live,* berisi jumlah router/hop maksimal yang boleh dilewati paket IP. Setiap kali paket IP melewati satu router, isi dari dield ini akan dikurangi satu. Jika time to live telah habis dan paket tetap belum sampai ke tujuan, paket ini akan dibuang dan router terakhir akan mengirimkan paket ICMP *time excedeed.* Hal ini dilakukan untuk mencegah paket IP terus menerus berada dalam network.
- *Protocol,* mengandung angka yang mengidentifikasikan protokol layer atas pengguna isi data dari paket IP ini.
- *Header Checksum,* berisi nilai *checksum* yang dihitung dari seluruh field dari *header* paket IP. Sebelum dikirimkan protokol IP terlebih dahulu menghitung *chencksum* dari header paket IP tersebut untuk nantinya dihitung kembali di sisi penerima. Jika ada perbedaan maka paket ini dianggap rusak dan dibuang
- *IP Address* pengirim dan penerima data, berisi alamat pengirim paket dan penerima paket.
- *Strict Source Route.* Berisi daftar lengkap IP Address dari router yang harus dilalui oleh paket ini dalam perjalanan ke host tujuan. Selain itu paket balasan atas paket ini yang mengalir dari host tujuan ke host

[1] Dosen STMIK PPKIA Pradnya Paramita Malang
[2] Dosen STMIK PPKIA Pradnya Paramita Malang

pengirim diharuskan melalui router yang sama.

- *Loose Source Route.* Dengan mengeset option ini paket yang dikirim diharuskan singgah di beberapa router seperti yang disebutkan di dalam field option.

Internet Control Message Protocol (ICMP)

Merupakan protokol yang bertugas mengirimkan pesan-pesan kesalahan dan kondisi lain yang memerlukan perhatian khusus. Paket/pesan ICMP dikirm jika terjadi masalah pada layer IP dan layer diatasnya (TCP/UDP)

Pada kondisi normal protokol IP berjalan baik dan menghasilkan proses penggunaan memori serta sumberdaya trnasmisi yang efisien. Namun ada beberapa kondisi dimana koneksi IP terganggu, misalnya karena router yang *crash,* putusnya kabel, atau matinya host tujuan. Pada saat ini ICMP berperan membantu menstabilkan kondisi jaringan. Hal ini dilakukan dengan cara memberikan pesan-pesan tertentu yang terjadi pada jaringan tersebut.

Ada dua jenis pesan yang dihasilkan oleh ICMP yaitu ICMP *error message* dan ICMP *query message.* ICMP *error message* sesuai dengan namanya dihasilkan jika terjadi kesalahan pada jaringan. Sedangkan ICMP *query message* ialah jenis pesan yang dihasilkan oleh protokol ICMP jika pengirim paket menginginkan informasi tertentu yang berkaitan dengan kondisi jaringan.

ICMP *error message* dibagi beberapa jenis, diantaranya adalah : *Destination unreachable,* pesan ini dihasilkan oleh router jika pengiriman paket mengalami kegagalan akibat masalah putusnya jalur, baik secara fisik maupun secara logis. *Destination unreachable* dibagi menjadi beberapa tipe antara lain :

1. *Network Unreachable,* jika jaringan tujuan tidak dapat dihubungi
2. *Host Unreachable,* jika host tujuan tidak bisa dihubungi.
3. *Protocol at Destination is Unreachable,* jika di tujuan tidak tersedia protokol tersebut.
4. *Port is Unreachable,* jika tidak ada port yang dimaksud pada tujuan.
5. *Destination Network is Unknow,* jika network tujuan tidak diketahui
6. *Destination Host is Unknow,* jika host tujuan tidak diketahui
7. *Time Exceeded,* paket ICMP jenis ini dikirimkan jika isi field TTL dalam paket IP sudah habis dan paket belum juga sampai ke tujuannya.

Sedangkan ICMP *Query Message* terdiri atas :

1. *Echo* dan *Echo Reply,* bertujuan untuk memeriksa apakah sistem tujuan dalam keadaan aktif. Program **ping** merupakan pengirim paket ini. Responden harus mengembalikan data yang sama dengan data yang dikirimkan.

[1] Dosen STMIK PPKIA Pradnya Paramita Malang
[2] Dosen STMIK PPKIA Pradnya Paramita Malang

2. *Time Stamp* dan *Timestamp Reply.* Menghasilkan informasi waktu yang diperlukan sistem tujuan untuk memproses suatu paket.
3. *Address Mask.* Untuk mengetahui berapa netmask yang harus digunakan oleh suatu host dalam suatu network

Address Resolution Protocol (ARP)

Dalam jaringan lokal, paket IP biasanya dikirm melalui card ethernet. Untuk berkomunikasi mengenali dan berkomunikasi dengan ethernet lainnya, digunakan ethernet address. Ethernet address ini besarnya 48 bit. Setiap card ethernet memiliki ethernet address yang berbeda-beda.

Pada saat hendak mengirimkan data ke komputer dengan IP tertentu suatu host pada jaringan ethernet perlu mengetahui ethernet address yang manakah tempat IP itu terletak. Untuk keperluan pemetaan IP address dengan ethernet address ini digunakan protokol ARP (*Address Resolution Protocol*)

ARP bekerja dengan mengirimkan paket berisi IP address yang ingin diketahui alamat ethernet-nya ke alamat broadcast internet. Karena dikirim ke alamat broadcast, semua card ethernet akan mendengar paket ini. Host yang merasa memiliki IP address ini akan membalas paket tersebut, dengan mengirimkan paket yang berisi pasangan IP address dan ethernet address. Untuk menghindari seringnya permintaan jawaban seperti ini, jawaban ini disimpan di memori (ARP Cache) untuk sementara waktu.

Transport Layer

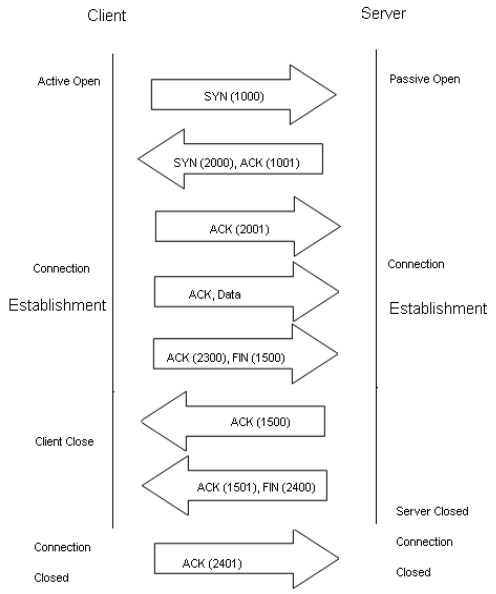
Transport Layer merupakan layer komunikasi data yang mengatur aliran data antara dua host, untuk keperluan aplikasi diatasnya. Ada dua buah protokol pada layer ini yaitu *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP).

Transmission Control Protocol (TCP)

TCP merupakan protokol yang terletak di layer transport. Protokol ini menyediakan service yang dikenal sebagai *connection oriented, reliable, byte stear service.*

Connection oriented berarti sebelum melakukan pertukaran data, dua aplikasi pengguna TCP harus melakukan pembentukan hubungan (*handshake*) terlebih dahulu. *Reliable* berarti TCP menerapkan proses deteksi kesalahan paket dan retransmisi. *Byte Strearm Service* berarti paket dikirimkan dan sampai ke tujuan secara berurutan.

[1] Dosen STMIK PPKIA Pradnya Paramita Malang
[2] Dosen STMIK PPKIA Pradnya Paramita Malang



Gambar 5 Pembentukan dan Pemutusan Koneksi TCP

Pada gambar 5 diatas adalah contoh yang sangat sederhana dari pembukaan hubungan TCP antara sebuah client dan server. Dapat kita lihat bahwa untuk memulai pembukaan suatu hubungan, client harus terlebih dahulu mengirimkan paket SYN (*Synchronize*). Setelah menerima paket tersebut server mengirimkan paket tersebut kembali. SYN miliknya serta *Acknowlwdge* (ACK) terhadap paket SYN sebelumnya. Saat client menerima paket ini, ia akan meng*acknowledge* serta mengirimkan data miliknya. Pada saat ini terbentuklah koneksi TCP antara dua komputer yaitu client dan server.

Angka dalam kurung yang mengikuti SYN pada gambar 5 diatas adalah representasi dari *sequence number*. *Sequence number* ini pada awalnya dihasilkan secara acak. Setiap *acknowledge* terhadap satu paket harus diikuti *sequence number* yang lebih tinggi dibanding *sequence number* sebelumnya. Untuk pemutusan hubungan TCP, kedua sisi harus mengirimkan paket yang berisi FIN (*finish*). Paket ini harus di *acknowledge* oleh lawan sebelum koneksi berakhir. Untuk menjamin kehandalan, TCP melakukan hal-hal berikut ini :

- Data yang diterima oleh aplikasi dipecah menjadi segmen-segmen yang besarnya menurut TCP paling sesuai untuk mengirimkan data.
- Ketika TCP menerima data dari mitranya, TCP mengirimkan *acknowledge* (pemberitahuan bahwa data telah diterima).
- Ketika TCP mengirimkan sebuah data, TCP mengaktifkan pewaktu (*software time*) yang akan menunggu *acknowledge* dari penerima segmen data tersebut. Jika sampai waktu yang ditentukan *acknowledge* tidak diterima, data tersebut akan dikembalikan ke TCP.
- Sebelum segmen data dikirim, TCP melakukan perhitungan *checksum* pada header dan datanya. Hal ini berbeda pada protokol IP yang hanya melakukan perhitungan pada headernya saja. Jika segmen yang diterima memiliki checksum yang tidak valid, TCP akan membuang segmen ini dan berharap sisi pengirim akan melakukan retransmisi.

[1] Dosen STMIK PPKIA Pradnya Paramita Malang
[2] Dosen STMIK PPKIA Pradnya Paramita Malang

- Karena segmen TCP dikirim menggunakan IP dan datagram IP dapat sampai ke tujuan dalam keadaan tidak berurutan, segmen TCP yang dikirimpun dapat mengalami hal yang sama. Karenanya sisi penerima paket TCP harus mampu melakukan pengurutan kembali segmen TCP yang ia terima (*resequencing*) dan memberikan data dengan urutan yang benar kepada aplikasi penggunanya.
- Karena paket IP dapat terduplikasi di perjalanan, penerima TCP harus membuang data tersebut.
- Untuk mencegah agar server yang cepat tidak membanjiri server yang lambat, TCP melakukan proses *flow control.* Setiap koneksi TCP memiliki *buffer* dengan ukuran yang terbatas. Sisi penerima TCP hanya memperbolehkan sisi pengirim data sebesar *buffer* yang ia miliki.

Bentuk segmen TCP terdapat pada gambar 6 berikut ini :

<table>
<tr><td colspan="3">Source Port</td><td>Destination Port</td></tr>
<tr><td colspan="4">Sequence Number</td></tr>
<tr><td colspan="4">Acknowledgement Number</td></tr>
<tr><td>Header</td><td>Resv</td><td>Control</td><td>Windows</td></tr>
<tr><td colspan="3">Checksum</td><td>Urgent Pointer</td></tr>
<tr><td colspan="4">TCP Option</td></tr>
</table>

Gambar 6 Format Segmen TCP

Segmen TCP terdiri atas beberapa field. *Source* dan *destination port* adalah field berisi angka yang mengidentifikasi aplikasi pengirim dan penerima sinyal segmen TCP ini. *Sequence number* berisi nomor urut byte stream dalam data aplikasi yang dikirim. Setiap kali data ini sukses dikirim, pihak penerima data mengisi *field acknowledgement number* dengan *sequence number* berikut yang diharapkan penerima.

Header length berisi header TCP, dengan lebar 4 bit. Field ini harus mempresentasikan panjang header TCP dalam satuan byte. Jika 4 bit ini berisi 1 (1111 biner = 15 desimal), maka panjang header maksimal ialah 15 x 4 = 60 byte.

User Datagram Protocol (UDP)

UDP memberikan suatu metoda kepada aplikasi untuk mengirim data ke aplikasi di host lain pada jaringan tanpa harus lebih dahulu membangun hubungan komunikasi dengan host tersebut (*connectionless*). UDP tidak menjamin keberhasilan pengiriman data (disebut sebagai datagram) tersebut dan tidak menjamin adanya duplikasi pengiriman.

Source dan *destination* digunakan sebagai identitas pengiriman dan karena UDP tidak memerlukan jawaban, maka *source port* sebenarnya tidak diperlukan. Port ini dalam pemrograman jaringan disebut sebagai socket. *Destination port* adalah nomor yang dikenal oleh aplikasi di mesin remote yang dijadikan identitas layanan. Sebagai contoh aplikasi FTP (*file transfer*) menggunakan nomor port 69. *Checksum*

[1] Dosen STMIK PPKIA Pradnya Paramita Malang
[2] Dosen STMIK PPKIA Pradnya Paramita Malang

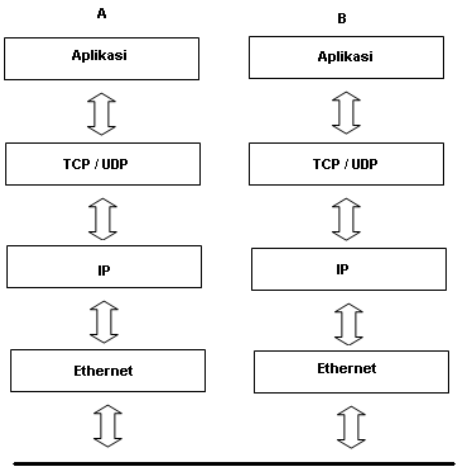
adalah satu-satunya mekanisme UDP untuk mendeteksi error pada pengiriman data.

Source Port	Destination Port
Datagram Length	Checksum
Application Data	

Gambar 7 Format Datagram UDP

Application Layer (Lapisan Aplikasi)

Lapisan aplikasi melayani permintaan pemakai untuk mengirim dan menerima data. Data ini kemudian disampaikan ke layer transport untuk diproses lebih lanjut. Konsep aplikasi digambarkan seperti pada gambar 8 berikut ini :



Gambar 8 Konsep Lapisan Aplikasi

4. Komponen Fisik dalam jaringan TCP/IP

Komputer dengan protokol TCP/IP dapat terhubung ke komputer lain dan jaringan lain karena bantuan peralatan jaringan komputer. Pada komputer itu sendiri, ditambahkan alat yang disebut *network interface. Network interface* ini bisa berupa *card ethernet* atau modem. Card ethernet terhubung ke komputer lain via kabel RG-58 atau ke hub ethernet via kabel UTP. Modem terhubung ke jaringan melalui kabel telepon. Di luar peralatan yang disebutkan ini, masih diperlukan peralatan lain untuk membentuk jaringan komputer. Peralatan ini disebut sebagai Device Penghubung Jaringan.

Device penghubung jaringan ini secara umum dibagi dalam beberapa kategori :

Repeater

Fasilitas paling sederhana dalam jaringan komputer adalah repeater. Fungsi utama dari repeater adalah menerima sinyal dari satu segmen kabel LAN dan memancarkannya kembali dengan kekuatan yang sama dengan sinyal asli pada segmen (satu atau lebih) kabel LAN yang lain. Dengan adanya repeater ini, jarak antara dua komputer bisa diperjauh.

Bridge

Sebuah bridge juga meneruskan paket dari satu segmen LAN ke segmen lain, tetapi bridge lebih flexibel dan lebih cerdas dibandingkan dengan repeater. Bridge bekerja dengan meneruskan paket ethernet dari satu jaringan ke jaringan lainnya. Tiap card ethernet memiliki alamat ethernet (*ethernet address*) yang unik. Beberapa bridge mempelajari alamat ethernet setiap device yang terhubung dengannya

[1] Dosen STMIK PPKIA Pradnya Paramita Malang
[2] Dosen STMIK PPKIA Pradnya Paramita Malang

dan mengatur alur frame berdasarkan alamat tersebut.

Bridge dapat menghubungkan jaringan yang menggunakan metode transmisi berbeda dan atau medium access control yang berbeda. Misalnya bridge dapat menghubungkan *ethernet baseband* dengan *ethernet broadband.* Bridge mungkin juga menghubungkan LAN Ethernet dengan LAN token ring, untuk mengisi ini, bridge harus mampu mengatasi perbedaan format paket setiap frame diatas.

Bridge mampu memisahkan sebagian trffic karena mengimplementasikan mekanisme pemfilteran (*frame filtering*). Mekanisme yang digunakan di bridge ini disebut sebagai *store and forward* sebab frame yang diterima disimpan sementara di bridge dan kemudian di foward ke workstation di LAN lain. Walaupun demikian *broadcast traffic* yang dibangkitkan dalam LAN tidak dapat difilter oleh bridge.

Router

Router memiliki kemampuan melewatkan paket IP dari satu jaringan ke jaringan lain yang mungkin memiliki banyak jalur diantara 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 satu sistem ke sistem lain.

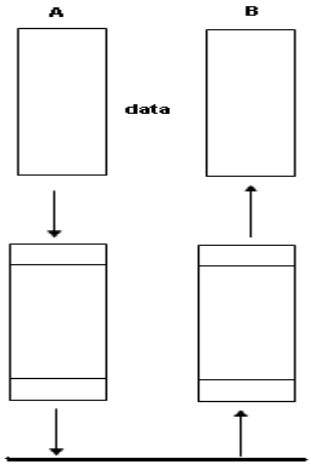
Router dapat digunakan untuk menghubungkan sejumlah LAN (*Local Area Network*) sehingga traffic yang dibangkitkan oleh suatu LAN terisolasikan dengan baik oleh traffic yang dibangkitkan oleh LAN lain. Jika dua atau lebih LAN terhubung dengan routerm setiap LAN dianggap sebagai subnetwork yang berbeda. Mirip dengan bridge, router dapat menghubungkan network interface yang berbeda.

Enkapsulasi

Data yang akan ditransfer oleh aplikasi diterima oleh protokol yang kemudian diberi tambahan berupa tanda pengenal, atau disebut header. Headre ini dapat terdiri atas 2 byte (16 bit), 4 byte (32 bit) atau berapa saja tergantung dari jenis protokol yang digunakan. Beberapa protokol bahkan memberikan informasi tambahan pada akhir data yang disebut *tailer.* Header dan tailer disebut sebagai pembungkus data dan kemudian setiap data yang dibungkus diberi nama paket. Teknik untuk mengendalikan informasi ini disebut sebagai *enkapsulation.* Header dan tailer dapat berisi informasi antara lain :

- Versi protokol
- Panjang data yang terkirim
- Tipe Protokol

[1] Dosen STMIK PPKIA Pradnya Paramita Malang
[2] Dosen STMIK PPKIA Pradnya Paramita Malang



Gambar 9 Enkapsulasi

IP Address

Sebagai pengguna internet, umumnya kita hanya perlu mengenal host name mesin yang dituju seperti server indo.net.id, rad.net.id, ui.net.id. Namun bagi komputer bekerja langsung dengan menggunakan informasi tersebut relatif sulit karena tidak ada keteraturan yang dapat diprogram dengan mudah. Untuk mengatasinya komputer mengidentifikasi alamat setiap komputer dengan sekumpulan angka sebanyak 32 bit yang dikenal dengan IP address.

IP address merupakan konsekuensi dari penerapan internet protokol (IP) untuk mengintergrasikan jaringan komputer internet di seluruh dunia. Seluruh host (komputer) yang terhubung ke internet dan ingin berkomunikasi memakai TCP/IP harus memiliki IP adrress sebagai alat pengenal host pada network, IP address harus bersifat unik untuk seluruh dunia, tidak boleh ada satu IP address yang sama dipakai oleh dua host yang berbeda.

IP address terdiri dari bilangan biner sepanjang 32 bit yang dibagi atas segment. Setiap segmen atas 8 bit yang berarti memiliki nilai desimal dari 0-255. IP address dapat dipisahkan menjadi 2 bagian yaitu bagia network (bit-bit network) dan bagian host (bit-bit host). Bit network berperan dalam identifikasi suatu network dari network yang lain. Sedangkan bit host berperan dalam identifikasi host dalam suatu metwork. Ada 3 kelas address yang utama dalam TCP/IP yakni Kelas A, B, dan C. Penentuan kelas ini dilakukan dengan cara berikut :

1. Jika bit pertama dari IP address adalah 0, address merupakan kelas network A. Bit ini dan 7 bit berikutnya (8 bit pertama) merupakan bit network sedangkan 24 bit terakhir merupakan bit host. Dengan demikian hanya ada 128 network kelas A, yakni dari 0 .xxx.xxx.xxx sampai 127 .xxx.xxx.xxx (xxx adalah variabel, nilainya dari 0 sampai dengan 255)
2. Jika 2 bit pertama dari IP address adalah 1 0, address merupakan kelas network B. Bit ini dan 14 bit berikutnya (16 bit pertama) merupakan bit network sedangkan 16 bit terakhir merupakan bit host. Dengan demikian terdapat lebih dari 16 ribu network kelas B, yakni dari network 128.0.xxx.xxx-sampai 191.255.xxx.xxx.

[1] Dosen STMIK PPKIA Pradnya Paramita Malang
[2] Dosen STMIK PPKIA Pradnya Paramita Malang

3. Jika 2 bit pertama dari IP address adalah 1 1 0, address merupakan kelas network C.3 bit ini dan 21 bit berikutnya (24 bit pertama) merupakan bit network sedangkan 8 bit terakhir merupakan bit host. Dengan demikian terdapat lebih dari 2 juta network kelas C, yakni dari network 192.0.0. xxx. Sampai 223.255..255 .xxx. setiap network C hanya mampu menampung sekitar 256 host.

Selain dari 3 kelas di atas, ada dua kelas lagi yang ditunjukkan untuk pemakaian khusus, yakni kelas D dan kelas E. Jika 4 bit pertama adalah 1 1 1 0, IP address merupakan kelas D yang digunakan untuk *multi cast address*, yakni sejumlah komputer yang memakai bersama suatu aplikasi (bedakan dengan pengertian *network address* yang mengacu pada sejumlah komputer yang memakai bersama suatu network). Salah satu penggunaan *multi cast address* yang berkembang saat ini di internet adalah untuk aplikasi *real time video conference* yang melibatkan lebih dari dua host (*multi point*). Menggunakan *multi cast back bone*. Kelas terakhir adalah kelas E (4 bit pertama adalah 1 1 1 1 atau siswa dari seluruh kelas). Pemakaiannya dicadangkan untuk kegiatan eksperimental.

HASIL DAN PEMBAHASAN

1. Instalasi Jaringan Internet

Yang pertama-tama harus dilakukan adalah instalasi jaringan internet dengan cara setting komputer agar terhubung dengan internet. Mula-mula hubungkan komputer dengan modem untuk menghubungkan ke pesawat telephon, kemudia setting *network neighborhood* pada windows alamat TCP/IP- nya.

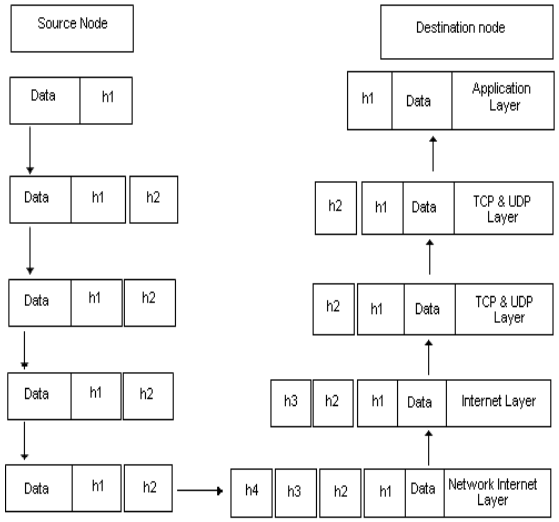
2. Transfer Data

Ada dua kegiatan dalam transfer data yaitu pengiriman dan penerimaan data. Pada sisi pengiriman data bergerak mulai dari lapisan TCP/IP yang paling atas yaitu : lapisan aplikasi, lapisan TCP dan UDP, lapisan internet dan terus bergerak sampai ke lapisan fisiknya. Saat data melewati setiap lapisan ini data akan mengalami perubahan-perubahan karena informasi yang ditambahkan (biasa disebut *Header Bits*) oleh setiap lapisan yang dilewatinya sebagai "pembungkus" data, agar sampai ke tujuan sesuai dengan yang dikirimkan. Guna memudahkan sebut saja h1, h2, h3, h4 (h=*Header Bits*). Saat data tiba pada lapisan bawah, data telah mengalami 4 kali penambahan termasuk dari *network interface layer* itu sendiri, kemudian data ini dikirimkan menuju *network interface layer* dari sisi penerima. Pada sisi penerima, pergerakan data adalah sebaliknya, yaitu data bergerak dari lapisan paling bawah sampai ke lapisan paling atas.

Dalam pergerakan data pada penerimaan ini, setiap informasi tambahan (*header bits*) pada data akan dihapus sesuai lapisan-lapisan pemberi informasi. Header bits yang diberikan oleh *network interface layer* pengiriman akan dihapus pada layer yang sama. Pada sisi penerima dan

[1] Dosen STMIK PPKIA Pradnya Paramita Malang
[2] Dosen STMIK PPKIA Pradnya Paramita Malang

begitu seterusnya hingga layer teratas dan data yang diterima sesuai dengan data yang dikirmkan oleh sisi pengiriman. Secara sederhana konsep pengiriman dan penrimaan data seperti pada gambar 10 berikut :



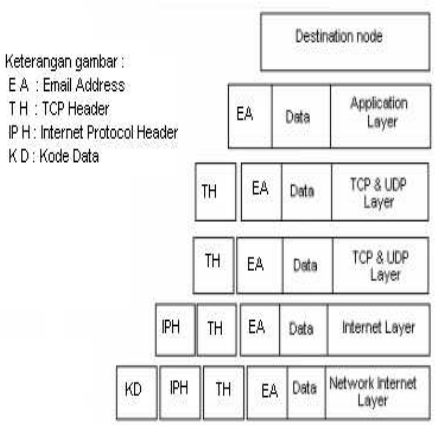
Gambar 10 Konsep Pengiriman dan Penerimaan Data

Keterangan : h1, h2, h3, h4 = header bits

Penerimaan Data

Pengambilan data melalui internet (*download*) yang seperti peneliti lakukan terlebih dahulu harus mengetikkan alamatnya. Dalam hal ini peneliti mengambil data pada http//www.google.com, selanjutnya membuka file mana yang akan didownload. Setelah itu kita panggil alamat yang hendak diambil datanya, setelah diambil datanya, maka data akan dikirimkan ke alamat yang kita maksud.

Pergerakan data dalam penerimaan data dapat dilihat pada gambar 11 berikut ini :



Gambar 11 Pergerakan Data dalam Penerimaan Data

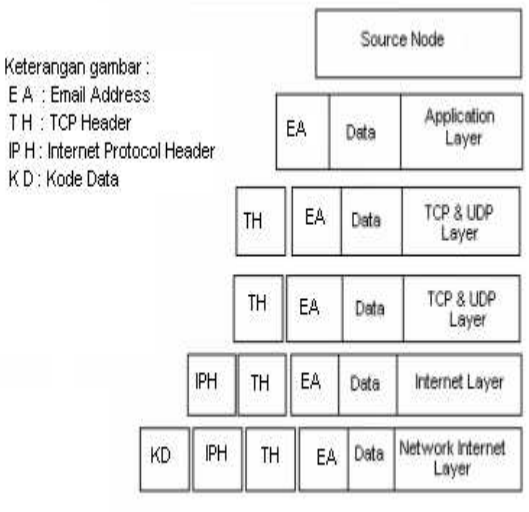
Penghapusan header pada tiap lapisan pada gambar diatas (sesuai dengan lapisan yang memberi headernya masing-masing header yang diberikan oleh lapisan IP pengiriman, maka akan dihapus pada lapisan IP pada penerimaan dan begitu juga pada setiap headernya.

Pengiriman Data

Untuk memindahkan data dari suatu tempat ke tempat lainnya dikerjakan oleh IP, begitu juga sebaliknya bila kita akan mengirimkan data ke suatu tujuan maka harus menentukan terlebih dahulu alamat dari tujuan tersebut. Sedangkan untuk transfer data tersebut maka akan dikerjakan oleh TCP dan IP seperti halnya pada proses pengambilan data, hanya saja pergerakan data pada pengiriman data adalah kebalikan alur gerak data penerimaan. Bila pada penerimaan header dihapus, sebaliknya pada pengiriman data yang hendak dikirm diberi header oleh setiap lapisan yang dilalui data itu.

[1] Dosen STMIK PPKIA Pradnya Paramita Malang
[2] Dosen STMIK PPKIA Pradnya Paramita Malang

Pergerakan data dalam pengiriman data dapat dilihat pada gambar 12 berikut ini :



Gambar 12 Pergerakan Data dalam Pengiriman Data

Untuk mengirim data ke tujuan TCP/IP, langkah-langkah yang harus ditempuh adalah sebagai berikut :

1. Datagram dibagi kedalam bagian-bagian terkecil yang sesuai dengan ukuran (*bandwith*) dimana data tersebut akan dikirimkan.
2. Pada lapisan TCP data tersebut lalu "dibungkus" dengan informasi header yang dibutuhkan. Misalnya cara mengarahkan data tersebut jika sampai pada tujuannya dan sebagainya.
3. Setelah datagram "dibungkus" dengan header TCP, datagram tersebut dikirimkan ke IP
4. IP menerima datagram dari TCP dan menambahkan headernya sendiri pada datagram tersebut.
5. IP lalu mengarahkan datagram tersebut ke tujuannya.
6. Komputer penerima melakukan proses perhitungan., untuk memastikan apakah data yang dikirim sama dengan data yang diterima.
7. Jika kedua perhitungan tersebut tidak cocok berarti ada error sewaktu pengiriman dan datagram akan dikirimkan kembali.

KESIMPULAN DAN SARAN

Kesimpulan

TCP/IP merupakan suatu protokol yang digunakan oleh para user untuk melakukan pengiriman dan penerimaan data. Pada sisi pengiriman data bergerak mulai dari lapisan TCP/IP yang paling atas, yaitu : lapisan aplikasi, lapisan TCP dan UDP, lapisan internet, dan terus bergerak sampai ke lapisan fisiknya. Saat data melewati setiap lapisan ini data akan mengalami perubahan-perubahan karena informasi yang ditambahkan (biasa disebut = *header bits*) oleh setiap lapisan yang dilewatinya sebagai "pembungkus" data, agar sampai ke tujuan sesuai dengan yang dikirmkan.

Dalam pergerakan data pada penerimaan ini, setiap informasi tambahan (*header bits*) pada data akan dihapus sesuai lapisan-lapisan pemberi informasi. *Header bits* yang diberikan oleh network interface layer pengiriman akan dihapus

[1] Dosen STMIK PPKIA Pradnya Paramita Malang
[2] Dosen STMIK PPKIA Pradnya Paramita Malang

pada layer yang sama. Pada sisi penerima begitu seterusnya hingga layer teratas dan data yang diterima sesuai dengan data yang dikirmkan oleh sisi pengiriman.

Saran-saran

Pada protokol TCP/IP pemberian alamat pada setiap komputer diharuskan berbeda-beda, hal ini digunakan untuk menghindari *crash system.* Di samping itu pula pada implementasi FTP, peneliti mengingatkan bahwa user diwajibkan untuk mengirimkan/memasukkan sebuah nama dan data khusus ke dalam server sebelum meminta transfer data.

DAFTAR PUSTAKA

Heywood, Drew, 1997, *Konsep dan Penerapan Microsoft TCP/IP,* Andi Offset, Yogyakarta.

Purbo, Onno W, 1998, *TCP/IP Standard Desain dan Implementasi,* PT. Elex Media Komputindo, Jakarta

----------, 1993, *Practical Internet Working With TCP/IP and UNIX.*

Sidharta, Lani, 1996, *Internet Informasi Bebas Hambatan I,* PT. Elex Media Komputindo, Jakarta

Suryadi, MT, 2000, *TCP/IP dan Internet sebagai Jaringan Komunikasi Data,* Andi Offset, Yogyakarta.

[1] Dosen STMIK PPKIA Pradnya Paramita Malang
[2] Dosen STMIK PPKIA Pradnya Paramita Malang

[1] Dosen STMIK PPKIA Pradnya Paramita Malang
[2] Dosen STMIK PPKIA Pradnya Paramita Malang