**MAKALAH**

**TCP/IP**

**MATA KULIAH : PERANCANGAN SISTEM JARINGAN KOMPUTER**



**Oleh:**

**Sandhitiyas Saiful Ma’arif**

**( L200130091)**

**UNIVERSITAS MUHAMMADIYAH SURAKARTA**

**FAKULTAS KOMUNIKASI DAN INFORMATIKA**

**2016**

**KATA PENGANTAR**

Syukur Alhamdulillah kehadirat Allah SWT yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan makalah yang merupakan salah satu Makalah mata kuliah Perancangan Sistem Jaringan Komputer t di Universitas Muhammadiyah Surakarta.

Makalah ini disusun dengan tema *TCP/IP*. Di dalam makalah ini terdapat penjelasan mengenai *TCP/IP* yang mudah dipahami.

Penulis menyadari bahwa makalah ini masih jauh dari sempurna. Karena itu, kritik dan saran yang bersifat konstruktif akan senantiasa penulis terima dengan senang hati. Dengan segala keterbatasan, penulis menyadari pula bahwa makalah ini tak akan terwujud tanpa bantuan, bimbingan dan dorongan dari berbagai pihak.

Semoga Allah SWT membalas kebaikan dan selalu mencurahkan hidayah serta taufikNya, Amin.

Surakarta,3 Maret 2012

                                                                                                       Penyusun

**DAFTAR ISI**

Halaman

Kata Pengantar i

Daftar Isi ii

Daftar Gambar iii

Daftar Tabel iv

Bab I Pendahuluan 1

1.1 Latar Belakang Masalah 1

1.2 Tujuan 1

1.3 Batasan Masalah 1

1.4 Manfaat 2

Bab II Tinjauan Pustaka 3

2.1 Sejarah TCP/IP 3

2.2 Organisasi Standar Internet 4

Bab III Pembahasan 5

3.1 *TCP*/*IP* Protocol Suite 5

3.2 Model *TCP/IP* Dan Osi 5

3.3 Arsitektur Jaringan *TCP/IP* 9

*A. Physical Layer* 9

*B. Network Access Layer* 9

*C. Internet Layer* 10

*D. Transport Layer* 21

*E. Application Layer* 21

3.4 Hubungan Antara Model Referensi *OSI* Dan *TCP/IP* 23

Bab IV Penutup 26

5.1 Kesimpulan 26

5.2 Saran 26

Daftar Pustaka 27

**DAFTAR GAMBAR**

Halaman

Gambar 3.1 Susunan Protokol TCP/IP dan model OSI 6

Gambar 3.2 Susunan Layer Protokol *TCP*/*IP* 6

Gambar 3.3 Susunan Protokol *TCP*/*IP* dan model OSI 7

Gambar 3.4 Aliran data protokol *TCP/IP* 8

Gambar 3.5 Enkapsulasi pesan ICMP 16

Gambar 3.6 Protocol ARP 19

Gambar 3.7 Enkapsulasi pesan ARP dalam frame jaringan 20

**DAFTAR TABEL**

Halaman

Tabel 3.1 Datagram Paket IP 12

Tabel 3.2 Jenis Pesan pada ICMP 17

Tabel 3.3 Susunan Protokol TCP/IP dan model OSI 24

**BAB I**

**PENDAHULUAN**

* 1. **LATAR BELAKANG MASALAH**

Dalam era globalisasi dan teknologi saat ini, penggunaan komputer sebagai salah satu alat teknologi informasi sangat dibutuhkan hampir disetiap perusahaan.

Penggunaan perangkat komputer sebagai perangkat pendukung manajemen dan pengolahan data adalah sangat tepat dengan mempertimbangkan kuantitas dan kualitas data, dengan demikian penggunaan perangkat komputer dalam setiap informasi sangat mendukung system pengambilan keputusan.

Dalam perkembangannya hingga pada jaringan, setiap perangkat komputer dapat berinteraksi dengan dengan komputer lainnya, dari jaringan lokal hingga jaringan global yang disebut internet.

* 1. **TUJUAN**

Adapun tujuan yang hendak dicapai dalam penulisan makalah ini adalah sebagai berikut :

1. Sebagai Tugas Mandiri (TM) mata kuliah Perancangan Sistem Jaringan Komputer pada program studi Teknik Informatika di Universitas Muhammadiyah Surakarta.
2. Sebagai masukkan bagi penulis untuk menambah wawasan khususnya mengenai *TCP*/*IP*.
   1. **BATASAN MASALAH**

Batasan masalah yang dapat diambil dari penulisan artikel ini adalah :

1. Sejarah *TCP*/*IP.*

2. Arsitektur *TCP/IP*.

3. Hubungan antara model arsitektur *OSI* dan *TCP/IP*

* 1. **MANFAAT**

Manfaat dari penulisan artikel ini adalah :

1. Lebih memahami tentang *TCP*/*IP* secara umum.

2. Lebih mendalami tentang arsitektur.

**BAB II**

**TINJAUAN PUSTAKA**

* 1. **SEJARAH TCP/IP**

Sejarah TCP/IP dimulainya dari lahirnya ARPANET yaitu jaringan paket switching digital yang didanai oleh DARPA (Defence Advanced Research Projects Agency) pada tahun 1969. Sementara itu ARPANET terus bertambah besar sehingga protokol yang digunakan pada waktu itu tidak mampu lagi menampung jumlah node yang semakin banyak. Oleh karena itu DARPA mendanai pembuatan protokol komunikasi yang lebih umum, yakni TCP/IP. Ia diadopsi menjadi standard ARPANET pada tahun 1983.

Untuk memudahkan proses konversi, DARPA juga mendanai suatu proyek yang mengimplementasikan protokol ini ke dalam BSD UNIX, sehingga dimulailah perkawinan antara UNIX dan TCP/IP. Pada awalnya internet digunakan untuk menunjukan jaringan yang menggunakan internet protocol (IP) tapi dengan semakin berkembangnya jaringan, istilah ini sekarang sudah berupa istilah generik yang digunakan untuk semua kelas jaringan. Internet digunakan untuk menunjuk pada komunitas jaringan komputer worldwide yang saling dihubungkan dengan protokol TCP/IP.

Perkembangan TCP/IP yang diterima luas dan praktis menjadi standar defacto jaringan komputer berkaitan dengan ciri-ciri yang terdapat pada protokol itu sendiri yang merupakan keunggulun dari TCP/IP, yaitu :

* Perkembangan protokol TCP/IP menggunakan standar protokol terbuka sehingga tersedia secara luas. Semua orang bisa mengembangkan perangkat lunak untuk dapat berkomunikasi menggunakan protokol ini. Hal ini membuat pemakaian TCP/IP meluas dengan sangat cepat, terutama dari sisi pengadopsian oleh berbagai sistem operasi dan aplikasi jaringan.
* Tidak tergantung pada perangkat keras atau sistem operasi jaringan tertentu sehingga TCP/IP cocok untuk menyatukan bermacam macam network, misalnya Ethernet, token ring, dial-up line, X-25 net dan lain lain.
* Cara pengalamatan bersifat unik dalam skala global, memungkinkan komputer dapat mengidentifikasi secara unik komputer yang lain dalam seluruh jaringan, walaupun jaringannya sebesar jaringan worldwide Internet. Setiap komputer yang tersambung dengan jaringan TCP/IP (Internet) akan memiliki address yang hanya dimiliki olehnya.
* TCP/IP memiliki fasilitas routing dan jenis-jenis layanan lainnya yangmemungkinkan diterapkan pada internetwork.
  1. **ORGANISASI STANDAR INTERNET**

Di bawah ini adalah beberapa organisasi yang *concern* dengan perkembangan standar teknologi telekomunikasi dan data internasional maupun dari Amerika.

* International Standards Organization (ISO).
* International Telecommunications Union-Telecommunication Standards Section (ITU - T).
* American National Standards Institute (ANSI).
* Institute of Electrical and Electronics Engineers (IEEE).
* Electronic Industries Association (EIA).

Selain itu terda pat pula organisasi yang bersifat forum ilmiah seperti Frame Relay Forum dan ATM Forum. Kemudian ada pula organisasi yang berfungsi sebagai agen regulasi, misalnya Federal Communications Commision (FCC).

**BAB III**

**PEMBAHASAN**

* 1. ***TCP*/*IP* PROTOCOL SUITE**

*TCP*/*IP* (singkatan dari *Transmission Control Protocol/Internet Protocol*) adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (*protocol suite*). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini. Data tersebut diimplementasikan dalam bentuk perangkat lunak (software) di sistem operasi. Istilah yang diberikan kepada perangkat lunak ini adalah *TCP*/*IP* stack

Protokol *TCP*/*IP* dikembangkan pada akhir dekade 1970-an hingga awal 1980-an sebagai sebuah protokol standar untuk menghubungkan komputer-komputer dan jaringan untuk membentuk sebuah jaringan yang luas (*WAN*). *TCP*/*IP* merupakan sebuah standar jaringan terbuka yang bersifat independen terhadap mekanisme transport jaringan fisik yang digunakan, sehingga dapat digunakan di mana saja. Protokol ini menggunakan skemapengalamatan yang sederhana yang disebut sebagai alamat *IP* (*IP* Address) yang mengizinkan hingga beberapa ratus juta komputer untuk dapat saling berhubungan satu sama lainnya di Internet. Protokol ini juga bersifat routable yang berarti protokol ini cocok untuk menghubungkan sistem-sistem berbeda (seperti Microsoft Windows dan keluarga *UNIX*).

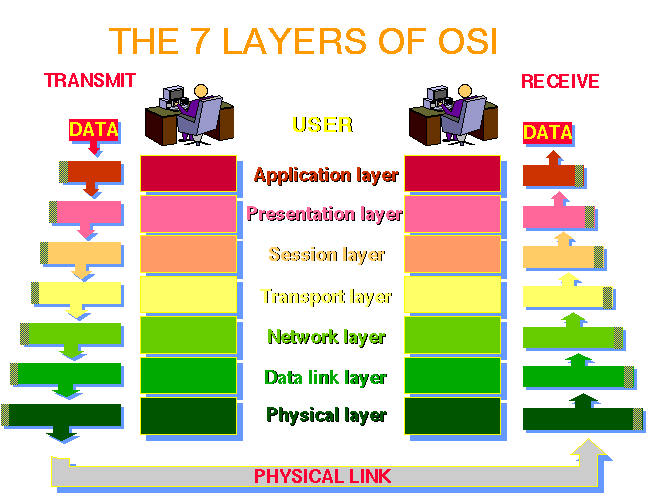
* 1. **MODEL *TCP/IP* DAN *OSI***

OSI = Open System Interconnection. adalah sebuah model jaringan yang dibuat oleh ISO. International Standards Organization. model ini terdiri dari 7 layer. Pada tiap layer tiap entitas saling berinteraksi dengan mengirimkan Protocol Data Unit (PDU). Tiap layer berhubungan dari layer atas ke bawahnya dengan mentransmisikan Servis Data Unit (SDU).

PDU pada masing-masing layer merupakan pesan lengkap yang mengimplementasikan protokol pada layer tersebut.

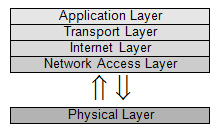
PDU pada OSI :

* layer1 = bit
* layer2 = frame
* layer3 = paket
* layer4 = segmen
* layer 5-7 = data

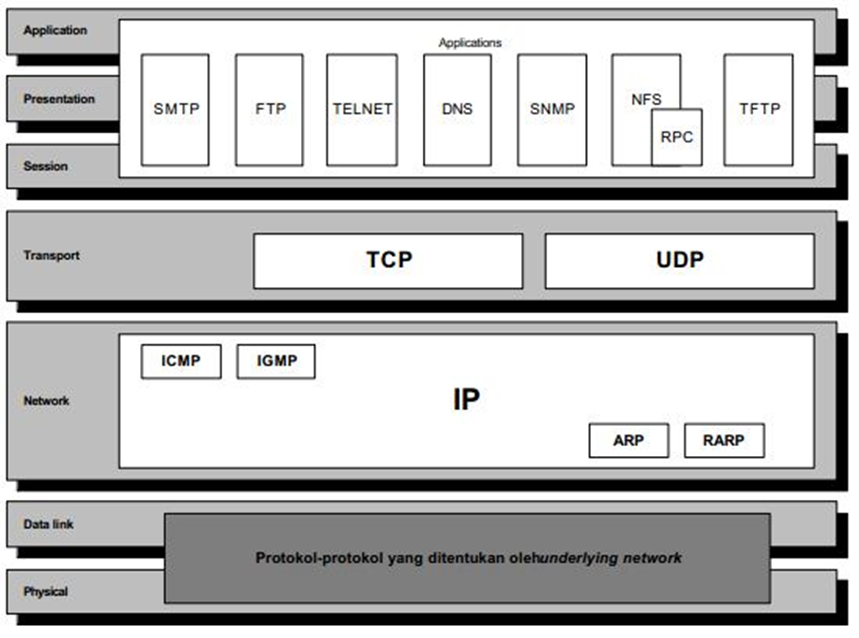


Gambar 3.1 Susunan Protokol *TCP*/*IP* dan model OSI

Model TCP/IP terdiri dari 5 layer yakni aplication layer, transport layer, internet layer, network access layer dan physical layer



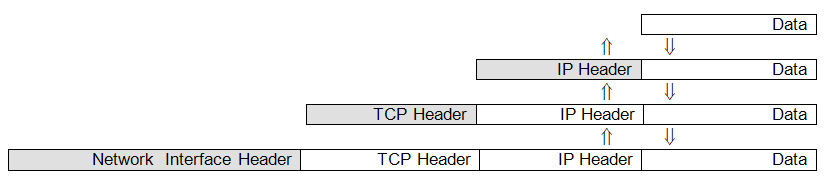
Gambar 3.2 Susunan Layer Protokol *TCP*/*IP*



Gambar 3.3 Susunan Protokol *TCP*/*IP* dan model OSI

Beberapa elemen konfigurasi umum TCP/IP dan tujuannya adalah sebagai berikut:

* IP address: IP address atau biasa disebut sebagai alamat IP merupakan sebuah string unik yang dituliskan dalam angka decimal yang dibagi dalam empat segmen. Tiap-tiap segmen bias ditulis angka yang terdiri atas 0 hingga 255. Tiap-tiap segmen tersebut merepresentasikan 8 bit dari alamat yang memiliki panjang 32 bit untuk keseluruhannya. Format ini disebut sebagai *dotted quad notation.*
* Netmask: subnet mask (biasa disingkat netmask) adalah tanda yang fungsinya membagi porsi dari alamat IP yang menunjukan Network dan porsi dari alamat IP yang menunjukan subnetwork. Misalnya untuk kategori alamat IP kelas C, netmask standard adalah 255.255.255.0, netmask tersebut berguna untuk masking 3 byte pertama dari alamat IP sementara byte terakhirnya disediakan untuk penentuan host subnetwork.
* Network address: network address merepresentasikan porsi jairngan dari alamat IP. Misalnya host 12.128.1.2 di jaringan kelas A memiliki network address 12.0.0.0. host jaringan yang menggunakan IP pribadi seperti 192.168.1.100 akan menggunakan network address 192.168.1.0. network address tersebut menjelaskan bahwa jaringan termasuk dibagian kelas C 192.168.1  network.
* Broadcast address: broadcast address merupakan alamat IP yang memungkinkan data jaringan dikirimkan secara simultan kesemua host subnetwork. Broadcast address standar untuk jaringan IP adalah 255.255.255.255. namun alamat broadcast ini tidak bisa digunakan untuk mem-Broadcast pesan kesemua host di internet karena adanya blok oleh router. Alamat broadcast biasanya di-set untuk subnetwork tertentu saja, semisal alamat IP 192.168.1.0. akan memiliki alamat broadcast 192.168.1.255. pesan broadcast biasanya dibuat oleh protokol jaringan seperti address resolution protocol (ARP) dan routing information protocol (RIP).
* Gateaway address: gateway address adalah alamat IP yang harus dilewati oleh semua komputer di jairngan ingin berkomunikasi dengan host dijairngan lain maka perlu adanya network gateaway. Dalam banyak kasus, gateaway address akan menjadi router di jaringan yang sama yang akan mengalokasikan traffic ke jaringan atau host lain (seperti internet).
* Nameserver address: nameserver address menunjukan IP address dari domain name service (DNS) yang bertujuan menerjemahkan nama hostname ke alamat IP. Ada tiga lapis nameserver yakni Primary Nameserver, Secondary Nameserver dan Tertiari Nameserver. Agar system anda resolve hostname dan menerjemeahkannya menjadi IP address, anda harus menentukan name server yang valid.



Gambar 3. 4 Aliran data protokol *TCP*/*IP*

Jika suatu protocol menerima data dari protocol lain di layer atasnya, ia akan menambahkan. Informasi tambahan miliknya ke data tersebut, Informasi ini memiliki fungsi yang sesuai dengan fungsi protocol tersebut. Setelah itu, data ini diteruskan lagi ke protocol pada layer di bawahnya. Hal yang sebaliknya terjadi jika suatu protocol menerima data dari protocol lain yang berada pada layer di bawahnya. Jika data ini dianggap valid, protocol akan melepas informasi tambahan tersebut untuk kemudian meneruskan data itu ke protocol lain yang berada pada layer di atasnya.

Device penguhubung jaringan ini secara umum dibagi menjadi beberapa kategori, yaitu:

* Repeater : Menerima sinyal dari satu segmen kabel LAN dan memancarkannya kembali.
* Bridge : Mirip Repeater namun lebih cerdas, karena bridge mempelajari setiap alamat Ethernet yang terhubung dengannya.
* Router : Memiliki kemampuan melewatkan paket IP dari satu jaringan ke jaringan lain yang mungkin memiliki banyak jalur diantara keduanya.

* 1. **ARSITEKTUR JARINGAN *TCP/IP***

Secara umum arsitektur jaringan *TCP/IP* dikelompokkan menjadi 5 layer yaitu aplication layer, transport layer, internet layer, network access layer dan physical layer.

1. **PHYSICAL LAYER**

Merupakan komponen fisik yang berupa media dan topologi.Ethernet, FDDI, ISDN, ATM.

1. **NETWORK ACCESS LAYER**

*Network Access Layer atau Network Interface Layer* merupakan gabungan antara *Network, Data Link* dan *Physical layer*. Lapis ini bertanggungjawab mengirim dan menerima data ke/dari media fisik. Media fisik bisa berupa kabel, serat optik atau gelombang radio, sehingga protocol ini harus mampu menerjemahkan sinyal listrik menjadi data digital yang dimengerti komputer yang berasal dari peralatan lain.

Protokol yang terdapat dalam layer ini adalah

* *PPP*(*Point to Point Protocol*) adalah protokol untuk point to point.
* *SLIP* (*Serial Line Internet Protocol*) adalah protokol dengan menggunakan sambungan serial.

1. **INTERNET LAYER**

*Internet Layer* bertanggung jawab dalam proses pengiriman paket ke alamat yang tepat. Dalam layer ini terdapat empat buah protocol yaitu :

1. ***IP* *(Internet Protocol)***

*IP* adalah protokol yang menyampaikan paket data ke alamat tujuan dengan tepat. Protokol *IP* merupakan inti dari protocol *TCP*/*IP*. Seluruh data yang berasal dari protocol pada layerdi atas *IP* harus dilewatkan oleh protocol *IP*, dan dipancarkan sebagai paket *IP*, agar sampai ke tujuan.

Dalam melakukan pengiriman data sampai ke alamat tujuan, *IP* memiliki sifat yaitu

1. *Unreliable*
2. *Connectionless,*
3. *Datagram delivery service*
4. *Unreliable*

*Unreliable* berarti bahwa Protokol *IP* tidak menjamin datagram yang dikirim pasti akan sampai ke tempat tujuan. Protokol *IP* hanya berjanji ia akan melakukan usaaha sebaik-baiknya (best effort delivery service), agar paket yang dikirim tersebut sampai ke tujuan. Jika di perjalanan terjadi hal-hal yang diinginkan (salah satu jalur putus, router down, atau host/network tujuan sedang down), protocol *IP* hanya memberitahukan ke pengirim paket melalui protocol *ICMP*, bahwa terjadi masalah dalam pengiriman paket *IP* ke tujuan. Jika diinginkan keandalan yang lebih baik, keandalan itu harus disediakan oleh protocol yang berada diatas layer *IP* ini (yaitu *TCP* dan application layer).

1. *Connectionless*

*Connectionless* berarti dalam mengirim paket dari tempat asal ke tujuan, pihak pengirim dan penerima paket *IP* sama sekali tidak mengadakan perjanjian (*handshake*) terlebih dahulu.

1. *Datagram delivery service*

Paket-paket data dalam protokol *IP* dikirimkan dalam bentuk datagram. Sebuah datagram *IP* terdiri atas header *IP* dan muatan *IP* (payload), sebagai berikut:

* *Header* *IP*: Ukuran header *IP* bervariasi, yakni berukuran 20 hingga 60 byte, dalam penambahan 4-byte. Header *IP* menyediakan dukungan untuk memetakan jaringan (routing), identifikasi muatan *IP*, ukuran header *IP* dan datagram *IP*, dukungan fragmentasi, dan juga *IP* Options.
* Muatan *IP*: Ukuran muatan *IP* juga bervariasi, yang berkisar dari 8 byte hingga 65515 byte.

*Datagram delivery service* berarti setiap paket data yang dikirim adalah independen terhadap paket data yang lain. Akibatnya jalur yang ditempuh oleh masing-masing paket data *IP* ke tujuannya bias jadi berbeda satu dengan yang lainnya. Karena jalur yang ditempuh berbeda, kedatangan paket pun bias jadi tidak berurutan. Hal ini dilakukan untuk menjamin tetap sampainya paket *IP* ke tujuan, walaupun salah satu jalur ke tujuan itu mengalami masalah.

Setiap paket *IP* membawa data yang terdiri atas :

* *Version*, berisi versi dari protocol yang dipakai. Saat ini yang dipakai ialah *IP* versi 4.
* *Header Length*, berisi panjang dari header paket *IP* dalam hitungan 32 bit word.
* *Type of Service*, berisi kualitas service yang dapat mempengaruhi cara pengangan paket *IP* ini.
* *Total Length of Datagram*, panjang *IP* datagram dalam ukuran byte.
* *Identification, Flags, dan Fragment Offset*, berisi beberapa data yang berhubungan dengan fragmentasi paket. Paket yang yang dilewatkan melalui berbagai jenis jalur akan mengalami fragmentasi ( dipecah menjadi beberapa paket yang lebih kecil) sesuai dengan besar data maksimal yang bias di transmisikan melalui jalur tersebut.
* *Time to Live,* berisi jumlah router/hop maksimal yang boleh dilewati paket *IP*. Setiap kali melewati satu router, isi dari field ini dikurangi satu. Jika *TTL* telah habis dan paket tetap belum sampai ke tujuan, paket ini akan dibuang dan router terakhir akan mengirimkan paket *ICMP time exceeded*. Hal ini dilakukan untuklmencegah paket *IP* terus menerus berada di dalam nerwork.
* *Protocol,* mengandung angka yang mengidentifikasikan protocol layer atas pengguna isi data dari paket *IP* ini.
* *Header Checksum*, berisi nilai *checksum* yang dihitung dari seluruh field dari header packet *IP*. Sebelum dikirimkan, protocol *IP* terlebih dahulu menghitung checksum dari header paket *IP* tersebut untuk nentinya dihitung kembali di sisi penerima. Jika terjadi perbedaan, maka paket ini dianggap rusak dan dibuang.
* *IP Address*  pengirim dan penerima data.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **VERSION** | **HEADER**  **LENGTH** | | **TYPE OF SERVICE** | | **TOTAL LENGTH OF DATAGRAM** |
| **IDENTIFICATION** | | **FLAG** | | **FRAGMENT OFFSET** | |
| **TIME TO LIVE** | | **PROTOCOL** | | **HEADER CHECKSUM** | |
| **SOURCE IP ADDRESS** | | | | | |
| **DESTINATION IP ADDRESS** | | | | | |
| **OPTIONS**  **STRICT SOURCE ROUTING, LOOSE SOURCE ROUTING** | | | | | |
| **DATA** | | | | | |

Tabel 3.1 Datagram Paket IP

*Internet Protocol* (*IP*) adalah mekanisme transmisi yang digunakan oleh *TCP*/*IP* yang sifatnya *unreliable* dan *connectionless*. Banyak yang mengistilahkan dengan *best effort delivery*, artinya: bahwa *IP* menyediakan *no error checking* atau *tracking* . Jika diperlukan reliabilitas maka *IP* mesti dipasangkan dengan protokol yang reliabel misalnya *TCP*. Contoh alama dari *IP* adalah, kantor pos mengirimkan surat tapi tidak selalu sukse dikirimkan. Jika surat tersebut tidak lengkap maka terserah pengirim ingin mengantarkannya atau tidak. Juga kantor pos tidak pernah menjejaki ke mana surat-surat yang jumlahnya jutaan itu terkirim.

*IP* Address ini dikelompokkan dalam lima kelas :

1. Kelas A

Format : 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh

Byte Pertama : 0 – 127 (127 untuk *local loopback*)

Jumlah : 126 kelas A ( 0 dan 127 dicadangkan )

*Range* *IP* : 1.xxx.xxx.xxx sampai 126.xxx.xxx.xxx

Jumlah *IP* : 16.777.214 *IP* Address untuk tiap kelas A

1. Kelas B

Format : 10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh

Byte Pertama : 128 – 191

Jumlah : 16384 kelas B

*Range* *IP* : 128.0.xxx.xxx sampai 191.155.xxx.xxx

Jumlah *IP* : 65.532 *IP* Address untuk tiap kelas B

1. Kelas C

Format : 110nnnn nnnnnnnn nnnnnnnn hhhhhhhh

Byte Pertama : 192 – 223

Jumlah : 2.097.152 Kelas C

*Range* *IP* : 192.0.0.xxx sampai 223.255.255.xxx

Jumlah *IP* : 254 *IP* Address untuk tiap kelas C

1. Kelas D

Format : 1110mmmm mmmmmmmm mmmmmmmm mmmmmmmm

Bit multicast : 128 bit

Byte Inisial : 224 – 247

Deskripsi : Kelas D adalah ruang alamat multicast (RFC 1112)

1. Kelas E

Format : 1111rrrr rrrrrrrr rrrrrrrr rrrrrrrr

Bit cadangan : 28 bit

Byte Inisial : 248 – 255

Deskripsi : Kelas D adalah ruang alamat yang dicadangkan untuk

keperluan eksperimental.

Ket : n = network bit, h = host bit, m = multicast bit, r = bit cadangan

1. ***ICMP* (Internet Control Message Protocol (*ICMP*)**

*ICMP* adalah salah satu protokol inti dari keluarga protokol internet. *ICMP* utamanya digunakan oleh sistem operasi komputer jaringan untuk mengirim pesan kesalahan yang menyatakan, sebagai contoh, bahwa komputer tujuan tidak bisa dijangkau.

Dalam suatu sistem connectionless setiap gateway akan melakukan pengiriman, perutean datagram yang dating 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, ttl dari counter habis, atau ketika terjadi kemacetan sehingga gateway tidak lagi bisa memproses paket yang datang.

Dalam koneksi dengan internet pengirim tidak dapat memberitahukan & tidak tahu sebab kegagalan suatu koneksi. Untuk mengatasinya diperlukan suatu metode yang mengijinkan 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 mengijinkan 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 & 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.

*Error & Query Reporting*

Secara teknis ICMP adalam 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 & kesalahan tujuan di intermediate gatewaynya maka tidak dapat dideteksi gateway mana yang gagal tersebut.

Ada beberapa jenis pesan error diantaranya :

* *Destination unreachable*

Pesan ini dihasilkan oleh router jika pengiriman paket mengalami kegagalan akibat masalah putusnya jalur, baik fisik maupun lojik.

Pesan ini dapat dibagi menjadi beberapa tipe :network

* *unreachable*

jika jaringan tujuan tidak dapat dihubungi

* *host unreachable*

jika host tujuan tidak bisa dihubungi

* *protocol at destination is unreachable*

jika di tujuan tidak tersedia protokol tersebut

* *port is unreachable*

jika tidak ada port yang dimaksud pada tujuan

* *destination network is unknown*

jika network tujuan tidak diketahui

* *destination host is unknown*

jika host tujuan tidak diketahui

* *Time exceeded*

Dikirimkan jika is field TTL dalam paket IP sudah habis masa aktifnya dan paket belum juga sampai ke tujuannya.

* *Parameter problem*

Pesan ini dikirim jika terjadi kesalahan parameter pada header paket IP.

* *Source quench*

Jika router atau tujuan mengalami kemacetan, sebagai respon terhadap pesan ini maka pihak penerima harus memperlambat pengiriman paket.

* *Redirect*

Dikirimkan jika router merasa host mengirimkan paket IP melalui router yang salah. Sedangkan untuk pesan query diantarannya adalah :

* *Echo & Echo Reply*

Bertujuan untuk memeriksa apakah sistem tujuan dalam keadaan aktif. Program ping merupakan program pengiriman paket ini. Responder harus mengembalikan data yang sama dengan data yang dikirimkan

* *Timestamp & Timestamp Reply*

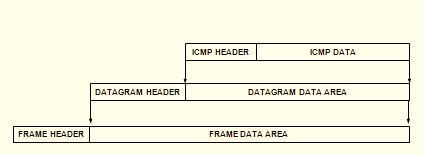
Menghasilkan informasi waktu yang diperlukan sistem tujuan untuk memproses suatu paket

* *Address Mask*

Untuk mengetahui berapa netmask yang harus digunakan oleh suatu host dalam suatu network.

***Pengiriman ICMP Message***

ICMP memerlukan dua level enkapsulasi. Setiap pesan ICMP merupakan bagian dari datagram IP yang juga merupakan bagain dari suatu frame data. Datagram yang membawa pesan ICMP mendapat perlakuan yang sama dengan datagram lain dalam hal reliability & priority-nya. Pengecualian prioritas didapat untuk menghindari masalah : mendapat pesan error mengenai pesan error. Prioritas tersebut menentukan bahwa pesan tidak dibangkitkan untuk error yang disebabkan oleh datagram yang membawa pesan error.



Gambar 3.5 Enkapsulasi pesan ICMP

***Format Pesan ICMP***

Format diawali dengan 3 field :

* 8 bit : field TYPE yang mengidentfikasikan pesan
* 8 bit : field CODE yang menyediakan informasi lebih jauh tentang tipe pesan
* 16 bit : field CHECKSUM untuk pengecekkan pesan ICMP

ICMP yang berisi pesan error terdiri dari header dan 64 bit pertamanya berisi penyebab error yang terjadi. Type field yang ada :

|  |  |
| --- | --- |
| **Type Field** | **ICMP Message Type** |
| 0 | Echo Reply |
| 3 | Destination Unreachable |
| 4 | Source Quench |
| 5 | Redirect (change a route) |
| 8 | Echo Request |
| 11 | Time Exceeded for a Datagram |
| 12 | Parameter Problem on a Datagram |
| 13 | Timestamp Request |
| 14 | Timestamp Reply |
| 15 | Information Request (obselete) |
| 16 | Information Reply (obsolote) |
| 17 | Address Mask Request |
| 18 | Address Mask Reply |

Tabel 3.2 Jenis Pesan pada ICMP

1. ***ARP (Adress 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*).

Ketika sebuah aplikasi yang mendukung teknologi protokol jaringan *TCP*/*IP* mencoba untuk mengakses sebuah host *TCP*/*IP* dengan menggunakan alamat *IP*, maka alamat *IP* yang dimiliki oleh host yang dituju harus diterjemahkan terlebih dahulu ke dalam *MAC Address* agar frame-*frame* data dapat diteruskan ke tujuan dan diletakkan di atas media transmisi (kabel, radio, atau cahaya), setelah diproses terlebih dahulu oleh *Network Interface Card (NIC).* Hal ini dikarenakan *NIC* beroperasi dalam lapisan fisik dan lapisan data-link pada tujuh lapis model referensi *OSI* dan menggunakan alamat fisik daripada menggunakan alamat logis (seperti halnya alamat *IP* atau nama *NetBIOS*) untuk melakukan komunikasi data dalam jaringan.

Jika memang alamat yang dituju berada di luar jaringan lokal, maka *ARP* akan mencoba untuk mendapatkan *MAC address* dari antarmuka router lokal yang menghubungkan jaringan lokal ke luar jaringan (di mana komputer yang dituju berada).g telah dikenal.

Protocol TCP/IP menggunakan pemetaan secara dinamik alamat IP ke alamat fisik level rendah. ARP hanya melalui jaringan tunggal dan terbatas ke jaringan yang mendukung adanya layanan broadcasting.

**Dua Tipe Alamat Fisik**

Ada dua tipe alamat fisik sebagai contoh : Ethernet yang memiliki alamat fisik yang besar & fix, serta proNET-10 yang memiliki konfigurasi alamat fisik yang kecil & mudah.

**Resolusi melalui Direct Mapping**

Untuk memilih skema yang membuat resolusi alamat yang efisien berarti memilih fungsi f yang memetakan alamat IP ke alamat fisik. Resolving alamat IP IA berarti

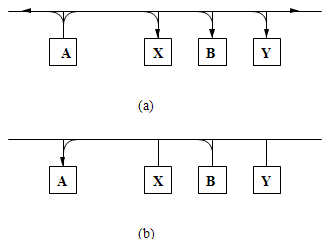
menghitung :

**PA = f(IA)**

Contoh : penggunaan X.25 yang tidak mengijinkan pemilihan alamat fisik. Biasanya gateway menyimpan pasangan alamat IP & fisik dalam satu tabel dan mencari dalam tabel ketika me-resolve suatu alamat IP. Fungsi Hash dapat digunakan untuk pencarian yang lebih efisien.

**Resolusi dengan Dynamic Binding**

Untuk kasus kesulitan resolusi alamat di suatu teknologi jaringan maka dapat digunakan suatu mesin ke jaringan tanpa adanya recompiling code dan tidak membutuhkan suatu pemeliharaan dari sebuah database terpusat. Untuk menghindari pemeliharaan tabel pemetaan, digunakan protocol level rendah yang dapat secara dinamik mem-binding alamat, yaitu ARP



Gambar 3.6 Protocol ARP

Ide dari metode ini adalah jika suatu host (A) ingin me-resolve suatu alamat (IB) maka A mem-broadcast paket khusus yang meminta host dengan alamat IP (IB)untuk meresponnya dengan alamat fisik PB. semua host termasuk B menerima request tetapi hanya host B yang mengenali alamat IP-nya & kemudian mengirim balasan(reply) yang berisi alamat fisik host B. ketika A menerim reply, A menggunakan alamat tersebut untuk mengirim paket internet secara langsung ke B.

**Address Resolution Cache**

Cache yanga ada dapat menyimpan pemetaan anatar alamat IP dengan alamat fisik sehingga pengiriman ARP secara berulang tidak diperlukan lagi. Pangisian cache dilakukan ketika pengirim menerima reply ARP.

**Implementasi ARP**

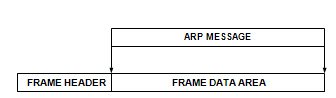
Secara fungsional penggunaan ARP dibagi menjadi 2 bagian :

* + - Bagian penentuan alamat fisik ketika mengirimkan sebuah paket
    - Bagian penjawab suatu request dari mesin lain.

Resolusi alamat untuk paket yang dikirimkan terlihat sederhana, ttetapi memiliki implementasi yang agak komplek. Ketika diberikan suatu alamat IP tujuan, host akan mengecek cache ARP-nya apakah pemetaan alamat tersebut sudah ada. Jika ada maka alamat fisik akan diproses, membentuk frame dengan alamat fisik yang didapat & mengirimkan frame tersebut. Tetapi jika alamat IP belum tercantum maka dikirimkan ARP secara broadcast & menunggu reply yang datang. Jika reply tidak datang karena mesin tujuan tidak aktif atau tertunda karena sibuk, maka dapat mengakibatkan request lost.

**Enkapsulasi & Identifikasi ARP**

Pesan ARP terkirim dalam bentuk frame dengan format :



Gambar 3.7 Enkapsulasi pesan ARP dalam frame jaringan

Untuk mengidentifikasi frame yang membawa request ARP atau reply ARP, pengirim harus menambahkan suatu nilai di header frame dan menempatkan pesan ARP dalam field datanya.

Contoh : frame yang membawa pesan ARP memiliki type field = 080616 yang merupakan nilai standar yang digunakan di Ethernet.

**Format Protokol ARP**

Paket ARP tidak memiliki format header yang tetap, karena di desain untuk dapat mendukung berbagai macam teknologi. Field pertama berisi count yang menentukan panjang field sesudahnya.

Terlihat 28 oktet pesan ARP yang digunakan di perangkat keras Ethernet ( dimana alamat fisik sepanjang 48 bit atau 6 oktet), ketika melalukan resolving alamat IP( panjang 4 oktet).

Di gambar juga terlihat pesan ARP dengan panjang 4 oktet per baris, suatu format yang sesuai dengan standarisasi.

1. ***RARP(Reverse Address Resolution Protocol)***

*RARP* merupakan sebuah protokol dalam *TCP*/*IP* yang berfungsi untuk mendapatkan alamat *IP* (alamat *Logic*) dengan menggunakan *MacAddress* (alamat *Physic*). *RARP* merupakan protokol yang memiliki fungsi kebalikan dari ARP. Keduanya memiliki fungsi sebagai resolutor alamat antara *Physic* dan *Logic*.

1. **TRANSPORT LAYER**

Transport layer mempunyai dua fungsi – mengatur aliran data antara dua host dan reliability.

Pada transport layer terdapat dua buah protocol :

* *TCP* -- *a connection-oriented,* reliable protocol, byte stream service. Connection Oriented berarti sebelum melakukan pertukaran data, dua aplikasi pengguna *TCP* harus melakukan hubungan (handshake) terlebih dahulu. Reliable berarti *TCP* menerapkan proses deteksi kesalahan paket dan retransmisi. Byte Stream Service berarti paket dikirimkan dan sampai ke tujuan secara berurutan.
* *UDP* -- *connectionless and unreliable.* Walaupun bertanggung jawab untuk mentransmisikan pesan/data, tidak ada software yang menge-cek pengantara setiap segmen yang dilakukan oleh layer ini. Keuntungan penggunaan UDP adalah kecepatannya karena pada UDP tidak ada acknowledgements, sehinggan trafik yang lewat jaringan rendah, dan itu yang membuat UDP lebih cepat daripada *TCP*.

Kegunaan UDP

* UDP cocok untuk proses yang memerlukan request-respons communication dan sedikit sekali memperhatikan masalah flow control dan error control.
* UDP yang melakukan proses dengan mekanisme internal flow control dan error control hanya untuk proses TFTP (Trivial File Transfer Protocol).
* UDP cocok untuk multicasting dan broadcasting pada lapisan transport.
* UDP digunakan untuk manajemen proses seperti aplikasi SNMP.
* UDP digunakan pengupdate protokol ruting seperti pada RIP (Routing Informastion Protocol).

1. **APPLICATION LAYER**

Pada sisi paling atas dari arsitektur protokol *TCP*/*IP* adalah Application Layer. Layer ini termasuk seluruh proses yang menggunakan transport layer untuk mengirimkan data. Banyak sekali application protocol yang digunakan saat ini.

Beberapa diantaranya adalah :

1. *TELNET,* yaitu *Network Terminal Protocol*, yang menyediakan remote login dalam jaringan.
2. *FTP*, *File Transfer Protocol*, digunakan untuk file transfer
3. FTP singkatan dari *File Transfer Protocol*. FTP merupakan mekanisme standar yang dimiliki Protokol TCP/IP untuk keperluan penyalinan (copying) file dari satu host ke host yang lain. FTP ini memanfaatkan layanan protokol TCP (lapisan 4) untuk melakukan operasinya.
4. *SMTP*, *Simple Mail Transfer Protocol*, digunakan untuk mengirimkan electronic mail.

SMTP adalah suatu protokol aplikasi yang merupakan sistem pengiriman *message*/pesan atau e-mail.

SMTP dapat mendukung 3 jenis pengiriman pesan:

* Pengiriman pesan saja kepada 1 atau lebih penerima.
* Pengiriman pesan yang termasuk dalamnya teks, suara, video atau grafik.
* Pengiriman pesan ke pengguna-pengguna yang di luar jaringan/internet.

Untuk melakukan operasinya SMTP memanfaatkan layanan protokol TCP (lapisan 4)

1. SNMP menyediakan sejumlah operasi fundamental untuk memonitor dan memelihara internet yang sudah besar organisasinya dan heterogen sifatnya. Konsep SNMP adalah *manager* dan *agent*. Selain itu SNMP memiliki komponen yakni : SMI (Structure of Management Information), MIB (Management Informastion Base) dan SNMP sendiri
2. *DNS*, *Domain Name Service*, untuk memetakan *IP* Address ke dalam nama tertentu. Untuk mengidentifikasi suatu entitas, protokol TCP/IP menggunakan alamat IP. Namun apabila dalam aplikasi setiap orang harus menghafal alamat IP untuk melakukan komunikasi bisa berakibat timbulnya kesulitan untuk mengingat. Apalagi jika perkembangan internet sudah demikian pesat. Untuk itiu protokol TCP/IP memiliki suatu metode untuk membuat suatu map yang menterjemhkan nama kepada alamat IP atau sebaliknya. Metode in i disebut juga sebagai *Domain Name System* (DNS).
3. *RIP*, *Routing Information Protocol*, protokol routing
4. *OSPF*, *Open Shortest Path First*, protokol routing
5. *NFS,* *Network File System*, untuk sharing file terhadap berbagai host dalam jaringan
6. *HTTP*, *Hyper Text Transfer Protokol,* protokol untuk web browsing.
   1. **HUBUNGAN ANTARA MODEL REFERENSI OSI DAN TCP/IP**

Hubungan antara model referensi OSI, TCP/IP dengan protocol internet yang digunakan.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NO** | **OSI** | **TCP/IP** | **Protokol Internet** | |
| **Layer** | **Layer** | **Nama Protokol** | **Fungsi** |
| 7 | Aplikasi | Aplikasi | DHCP(*Dynamic Host Configuration Protocol*) | Protokol untuk distribusi IP pada jaringan dengan jumlah terbatas |
| FTP*(File Transfer Protocol*) | Protokol untuk transfer file |
| HTTP (*Hyper Text Transfer Protocol*) | Protokol untuk transfer file html dan web |
| MIME(*Multipurpose Internet Mail Extention*) | Protokol untuk mengirim file *binary* dalam bentuk teks |
| POP (*Post Office Protocol*) | Protokol untuk mengambil mail dari server |
| SMB (*Server Message Board*) | Protokol untuk transfer berbagai server file DOS dan Windows |
| 6 | Presentasi | SMTP (*Simple Mail Transfer protocol*) | Protokol untuk pertukaran mail |
| SNMP(*Simple Network Management Protocol*) | Protokol untuk manajemen jaringan |
| TELNET | Protokol untuk akses jarak jauh |
| TFTP(*Trivial FTP*) | Protokol untuk transfer file |
| 5 | Session | NETBIOS(*Network Basic Input Output System*) | BIOS untuk jaringan standar |
| RPC(*Remote Procedure Call*) | Prosedur pemanggilan jarak jauh |
| SOCKET | Input Output untuk *network* jenis BSD UNIX |
| 4 | Transport | Transport | TCP (trasmision Control protokol | Protokol untuk pertukaran data berorientasi (connected orientasi) |
| 3 | Network | Internet | IP(Internet Protokol) | Protokol untuk menetapkan routing |
| RIP *(Routing Information Protocol)* | Protokol untuk memilih routing |
| ARP*(Address Resolution Information Protocol)* | Protokol untuk mendapatkan informasi hardware dari nomor IP |
| RARP*(Reverse Address Resolution Information Protocol)* | Protokol untuk mendapatkan informasi nomor IP dari hardware |
| 2 | Datalink | Network Interface | PPP*( Point to point Protocol)* | Protokol untuk point to point |
| SLIP*( Serial Line Internet Protocol)* | Protokol dengan menggunakan sambungan serial |
| 1 | Fisik | Ethernet, FDDI, ISDN, ATM | |

Tabel 3.3 Susunan Protokol TCP/IP dan model OSI

Persamaan model OSI dan model TCP/IP

* Keduanya memiliki layer(lapisan)
* Sama-sama memiliki Application Layer meski layanannya berbeda.
* Memiliki transport network layer yang sama

Perbedaan model OSI dan model TCP/IP

* TCP/IP mengkombinasikan presentation layer dan session layer pada lapisan aplikasi.
* TCP/IP menggabuungkan Data Link dan Physical layer menjadi satu lapisan

**BAB IV**

**PENUTUP**

**4.1 KESIMPULAN**

Sesuai dengan penjabaran penulis pada bab – bab sebelumnya, maka penulis akan mencoba untuk menyimpulkan mengenai makalah yang disusun. Berikut ini kesimpulan tersebut adalah sebagai berikut :

1. *TCP*/*IP* merupakan sebuah paket protokol yang berfungsi sebagai metode dalam komunikasi antar komputer atau node.
2. *TCP*/*IP* diimplementasikan dalam bentuk perangkat lunak (Software) yang ada dalam sebuah Sistem Operasi.
   1. **SARAN**

Setelah menyusun makalah ini penulis memiliki harapan untuk mata kuliah Jaringan Komputer Jaringan. Berikut ini saran dari penulis:

* Seharusnya mata kuliah Jaringan Komputer dan Internet di lengkapi dengan praktek di Laboratorium.
* Adanya video simulasi di setiap bab yang dibahas.

**DA FTAR PUSTAKA**

Maslan, A. (2012). *Teori, Praktek dan Simulasi Jaringan Komputer dan Internet.* Jakarta: Baduose Media.

Tharom, T. (2002). *Mengenal Teknologi Informasi.* Jakarta: Elex Media Komputindo.

Wikipedia. (2012, 12 28). *id.wikipedia.org*. Retrieved 12 2012, 1, from wikipedia.org: id.wikipedia.org/wiki/Internet\_protocol\_suite

Winarno, S. (2010). *Jaringan Komputer TCP/IP.* Bandung: Modula.

Dani. (2011, 05 20). *blackheart*. Retrieved 12 1, 2012, from daniblackheart.blogspot.com: http://daniblackheart.blogspot.com/2011/05/makalah-tcp-ip.html

Irwan. (2009, 04 30). *web.itb.ac.id*. Retrieved from itb.ac.id: web.itb.ac.id/irwan/data/.../4-Introduction%20TCP%20-%20IP.doc