

## BAB II

# INTERNET PROTOCOL

Dalam melakukan pengiriman data protokol IP memiliki sifat yang dikenal sebagai unreliable, connectionless, datagram delivery service.

Unreliable atau ketidakhandalan berarti tidak ada jaminan sampainya data di tempat tujuan. Connectionless berarti dalam mengirim paket dari tempat asal ke tujuan, tidak diawali dengan perjanjian (handshake) antara pengirim & penerima. Sedangkan datagram delivery service berarti setiap paket data yang dikirim adalah independen terhadap paket data yang lain. Jalur yang ditempuh antara satu data dengan yang lain bisa berbeda. Sehingga kedatangannya pun bisa tidak teratur seperti urutan pengiriman.

Dalam mengirim data, protokol IP memiliki format datagram khusus sebagai berikut :

<b>VERSION</b>	<b>HEADER LENGTH</b>	<b>TYPE OF SERVICE</b>	<b>TOTAL LENGTH OF DATAGRAM</b>	
<b>IDENTIFICATION</b>			<b>FLAG</b>	<b>FRAGMENT OFFSET</b>
<b>TIME TO LIVE</b>	<b>PROTOCOL</b>		<b>HEADER CHECKSUM</b>	
<b>SOURCE IP ADDRESS</b>				
<b>DESTINATION IP ADDRESS</b>				
<b>OPTIONS</b> <b>STRICT SOURCE ROUTING, LOOSE SOURCE ROUTING</b>				
<b>DATA</b>				

Gambar format datagram IP

Version untuk menunjukkan versi protokol yang dipakai, Header Length menunjukkan panjang paket header dalam hitungan 32 bit. Type of Service menunjukkan kualitas layanan, Total Length of datagram menunjukkan total keseluruhan panjang datagram. Identification, Flags & Fragment Offset digunakan untuk fragmentasi paket, TTL menunjukkan jumlah hop maksimal yang dilewati paket IP.

Sedangkan Protocol mengandung angka yang mengidentifikasi protokol layer atasnya. Header Checksum untuk mengecek kebenaran isi header datagram. Source & destination IP Address merupakan alamat pengirim dan penerima datagram. Untuk byte

option dapat berisi Strict Source Route, yaitu daftar lengkap alamat IP dari router yang harus dilalui untuk sampai ke tujuan, dan Loose Source Route.

## **2.1 PENGALAMATAN**

### **2.1.1 Identifikasi Universal**

Suatu sistem komunikasi dikatakan mampu menyediakan layanan komunikasi universal jika di dalam sistem tersebut setiap host dapat berkomunikasi dengan seluruh host yang ada dalam sistem tersebut. Untuk dapat berkomunikasi diperlukan suatu metode global pengenalan host yang dapat diterapkan disemua host yang ada.

Seringkali metode identifikasi host menggunakan *name*, *addresses* atau *routes*. Dimana *name* mengidentifikasi apa nama objek tersebut, *addresses* mengidentifikasi dimana objek tersebut berada dan *routes* mengidentifikasi bagaimana untuk bisa sampai di objek tersebut.

### **2.1.2 Format Alamat IP**

#### ***Bentuk Biner***

Alamat IP merupakan bilangan biner 32 bit yang dipisahkan oleh tanda pemisah berupa tanda titik setiap 8 bitnya. Tiap 8 bit ini disebut sebagai oktet. Bentuk alamat IP adalah sebagai berikut :

XXXXXXXX.XXXXXXXXXX.XXXXXXXXXX.XXXXXXXXXX

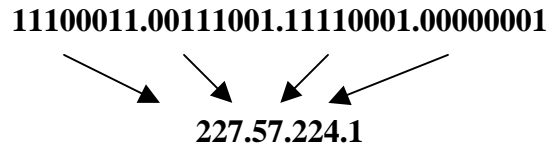
setiap symbol “x” dapat digantikan oleh angka 0 dan 1, misalnya sebagai berikut :

**11100011.00111001.11110001.00000001**

#### ***Bentuk Dotted Desimal***

Notasi alamat IP dengan bilangan biner seperti di atas tidaklah mudah dibaca. Untuk membuatnya lebih mudah dibaca & ditulis, alamat IP sering ditulis sebagai 4 bilangan desimal yang masing-masing dipisahkan oleh sebuah titik. Format penulisan seperti ini disebut “*dotted-decimal notation*” (notasi desimal bertitik). Setiap bilangan desimal tersebut merupakan nilai dari satu oktet (delapan bit) alamat IP. Gambar

berikut memperlihatkan bagaimana sebuah alamat IP yang ditulis dengan notasi dotted-desimal :



gambar Notasi Dotted-Decimal

### **2.1.3 Pengalamatan untuk Koneksi Jaringan Khusus**

Seperti telah disebutkan sebelumnya, alamat IP digunakan untuk mengidentifikasi suatu host. Kemudian timbul pertanyaan bagaimana suatu pengalamatan suatu gateway yang terhubung banyak koneksi ?, tentu saja tidak bisa menggunakan satu alamat IP.

*Multi-homed address & gateway* memerlukan alamat-alamat IP yang berbeda. Setiap alamat mengidentifikasi koneksi yang berbeda. Jadi suatu alamat IP bukan untuk mengidentifikasi suatu host individu melainkan mengidentifikasi suatu koneksi di jaringan meliputi mengidentifikasi jaringan dan host yang terhubung. Untuk n koneksi, suatu gateway memiliki n alamat IP.

### **2.1.4 Pengalamatan Jaringan & Broadcast**

Keuntungan dari pengkodean informasi jaringan di alamat internet adalah untuk mendapatkan perutean yang efisien. Keuntungan lain yang didapat adalah alamat internet dapat mengacu ke jaringan yang dipakai sebaik pengacuan ke suatu host. Sebagai contoh semua bit pada hostid bernilai 0 tidak akan pernah digunakan untuk menandai suatu host, melainkan untuk menandai suatu jaringan.

Contoh lain, jika semua bit pada hostid bernilai 1 maka berarti pengalamatan untuk semua host di jaringan tersebut (broadcast).

### **2.1.5 Pengalamatan Broadcast Terbatas**

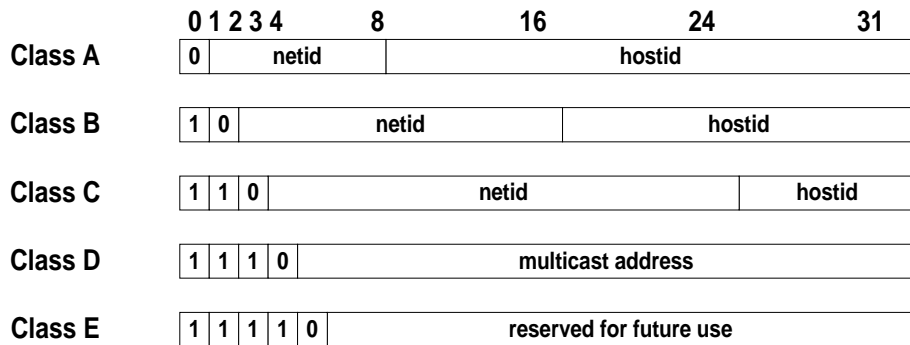
Pengalamatan ini menyediakan suatu alamat broadcast untuk jaringan lokal yang tidak tergantung pada alamat IP. Alamat broadcast local terdiri dari 32 bit dengan nilai 1.

Suatu host dapat menggunakan alamat broadcast terbatas ini sebagai bagian dari prosedur start-up sebelum mempelajari alamat IP atau

## **2.2 KLASIFIKASI**

Setiap host yang terhubung di jaringan internet memiliki alamat internet unik sebanyak 32 bit yang digunakan untuk berkomunikasi dengan semua host.

Setiap alamat yang ada terdiri dari sepasang *netid & hostid*. *Netid* mengidentifikasi jaringan yang dipakai dan *hostid* mengidentifikasi host yang terhubung ke jaringan tersebut. Ada beberapa macam alamat berdasarkan kelas yang ada :



gambar kelas-kelas alamat IP

Keterangan :

Kelas A :

Format : 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh  
 Identifikasi : bit pertama 0  
 Panjang NetID : 8 bit  
 Panjang HostID : 24 bit  
 Byte pertama : 0 – 127  
 Jumlah jaringan : 126 kelas A (0 dan 127 dicadangkan)  
 Range IP : 1.xxx.xxx.xxx sampai 126.xxx.xxx.xxx  
 Jumlah IP : 16.777.214 alamat IP pada setiap kelas A

Kelas B

Format : 0nnnnnnn nnnnnnnn hhhhhhhh hhhhhhhh  
 Identifikasi : 2 bit pertama 10  
 Panjang NetID : 16 bit  
 Panjang HostID : 16 bit  
 Byte pertama : 128 – 191  
 Jumlah jaringan : 16.384 kelas B  
 Range IP : 128.0.xxx.xxx sampai 191.155.xxx.xxx  
 Jumlah IP : 65.532 alamat IP pada setiap kelas B

Kelas C

Format : 0nnnnnnn nnnnnnnn nnnnnnnn hhhhhhhh  
 Identifikasi : 3 bit pertama bernilai 110  
 Panjang NetID : 24 bit  
 Panjang HostID : 8 bit  
 Byte pertama : 192 – 223  
 Jumlah jaringan : 2.097.152 kelas C  
 Range IP : 192.0.0.xxx sampai 223.255.255.xxx  
 Jumlah IP : 254 alamat IP pada setiap kelas C

Kelas D

Format : 1110mmmm mmmmmmmm mmmmmmmm mmmmmmmm  
 Identifikasi : 4 bit pertama bernilai 1110  
 Bit multicast : 28 bit  
 Byte Inisial : 224 - 247 bit  
 Deskripsi : Kelas D adalah ruang alamat multicast (RFC 1112)

#### Kelas E

Format : 1111rrrr rrrrrrrr rrrrrrrr rrrrrrrr  
 Identifikasi : 4 bit pertama 1111  
 Bit cadangan : 28 bit  
 Byte inisial : 248 –255  
 Deskripsi : Kelas E adalah ruang alamat yang dicadangkan untuk keperluan eksperimental

Dari macam-macam bentuk alamat IP, setiap kelas dapat diidentifikasi dari 3 bit tertinggi dengan dua bit menjadi pembeda tiga kelas utama. Kelas A digunakan untuk jaringan besar dengan  $2^{16}$  host terhubung kepadanya. Untuk kelas A, 7 bit untuk netid dan 24 bit untuk hostid. Kelas B untuk jaringan berukuran sedang, dengan daya tampung antara  $2^8$  sampai  $2^{16}$  host. Kelas B mengalokasikan 14 bit untuk netid & 16 bit untuk hosted. Kelas C mampu menghubungkan kurang dari  $2^8$  host dengan mengalokasikan 21 bit untuk netid dan hanya 8 bit untuk hostid.

## 2.3 ROUTING

### 2.3.1 Routing di Internet

Dalam suatu sistem packet switching, routing mengacu pada proses pemilihan jalur untuk pengiriman paket, dan router adalah perangkat yang melakukan tugas tersebut.

Perutean dalam IP melibatkan baik gateway maupun host yang ada. Ketika suatu program aplikasi dalam suatu host akan berkomunikasi, protocol TCP/IP akan membangkitkannya dalam bentuk banyak datagram. Host harus membuat keputusan perutean untuk memilih jalur pengiriman.

### 2.3.2 Pengiriman Langsung & Tidak Langsung

Pengiriman langsung (*direct delivery*) adalah transmisi datagram dari suatu mesin langsung ke mesin lain, dan hal ini dapat terjadi bila keduanya berada dalam satu media

transmisi yang terhubung langsung. Sedangkan pengiriman yang tidak langsung mengharuskan suatu datagram untuk melewati gateway.

Untuk pengiriman langsung datagram IP, pengirim akan mengenkapsulasi datagram dalam suatu frame fisik, memetakan alamat IP tujuan ke alamat fisik dan menggunakan perangkat keras jaringan untuk pengiriman secara langsung.

Identifikasi bahwa tujuan masih berada dalam satu jaringan dapat dilihat di alamat IP bagian network-nya, jika ditemukan alamat yang sama maka dapat dilakukan pengiriman langsung.

Pengiriman tidak langsung terjadi bilamana antar host yang bertukar informasi tidak terletak pada satu jaringan sehingga perlu melalui beberapa gateway hingga gateway terakhir dapat dicapat dan pengiriman langsung dapat dilakukan.

### 2.3.3 Table Routing

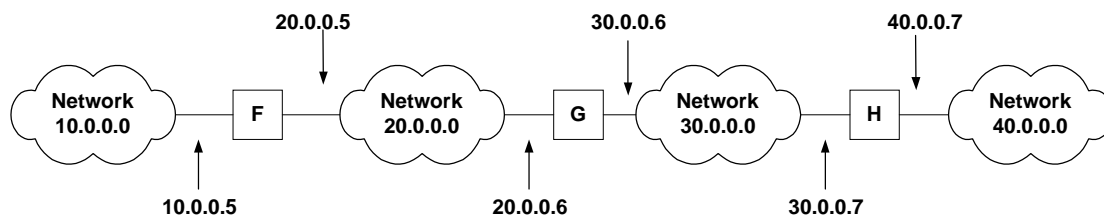
Suatu algoritma perutean menggunakan table perutean yang menyimpan informasi mengenai kemungkinan tujuan yang dapat dicapai & cara pencapaiannya. Karena baik host maupun gateway merutekan datagram, maka keduanya memiliki table perutean.

Untuk pengefisienan table routing tidak semua informasi mengenai kemungkinan tujuan akan disimpan. Alamat IP-pun tidak perlu ditulis lengkap

Biasanya tabel routing terdiri dari pasangan Network & Gateway (N,G) dimana N menunjukkan jaringan tujuan & G merupakan gateway berikutnya untuk sampai di jaringan N.

Tabel perutean akan selalu menunjuk ke gateway yang dapat ditempuh langsung dalam satu jaringan. Semua gateway yang terdaftar di mesin tabel perutean mesin M harus terletak dalam satu jaringan. Ketika suatu datagram akan meninggalkan mesin M maka perangkat lunak IP akan mencari alamat IP tujuan dan menggunakan bagian networknya untuk membuat keputusan perutean, pemilihan gateway dan pengiriman secara langsung.

Contoh :



Ada 4 jaringan dengan 3 gateway yang menghubungkannya. Pada gambar di atas bila gateway G memiliki tabel perutean maka berisi :

JARINGAN YANG DICAPAI	ALAMAT YANG DILEWATI
20.0.0.0	DELIVER DIRECTLY
30.0.0.0	DELIVER DIRECTLY
10.0.0.0	20.0.0.5
40.0.0.0	30.0.0.7

Ukuran tabel routing tergantung pada jumlah jaringan yang terhubung. Kapasitasnya akan bertambah jika jumlah jaringan yang terhubung bertambah tanpa tergantung pada host yang terhubung.

Metode lain untuk menghemat ukuran tabel routing adalah menjadikan masukkan-masukkan tertentu dalam bentuk **default**. Prinsip dari metode ini : perangkat lunak IP akan melihat dahulu isi tabel routing untuk jaringan tujuan, jika tidak ada jalur yang terlihat dalam tabel maka dikirimkan datagram ke default gateway.

Metode ini sangat berguna untuk jaringan dengan jumlah alamat local tidak terlalu banyak & hanya satu koneksi menuju internet.

### 2.3.3.1 Proses Pencarian dalam Tabel Routing

Proses pencarian pada tabel routing ini biasanya mengikuti langkah-langkah dibawah ini :

1. Alamat tujuan datagram di-masking dengan subnet mask host pengirim dan dibandingkan dengan alamat network host pengirim. Jika sama, maka ini adalah routing langsung dan frame langsung dikirimkan ke interface jaringan
2. Jika tujuan datagram tidak terletak dalam satu jaringan, periksa apakah terdapat entri routing yang berupa host dan bandingkan dengan alamat IP tujuan datagram. Jika ada entri yang sama, kirim frame ke router menuju host tersebut.
3. jika tidak terdapat entri host yang cocok pada tabel routing, gunakan alamat tujuan datagram yang telah di-mask pada langkah 1 untuk mencari kesamaan di tabel routing. Periksa apakah ada network/subnetwork di tabel routing yang

sama dengan alamat network tujuan datagram. Jika ada entri yang sama, kirim frame ke router menuju network/subnetwork tersebut.

4. jika tidak terdapat entri host ataupun entri network/subnetwork yang sesuai dengan tujuan datagram, host mengirimkan frame ke router default dan menyerahkan proses proses routing selanjutnya kepada router default.
5. Jika tidak terdapat rute default di tabel routing, semua host diasumsikan dalam keadaan terhubung langsung. Dengan demikian host pengirim akan mencari alamat fisik host tujuan menggunakan ARP

### **2.3.3.2 Membentuk Tabel Routing**

Ketika suatu host baru dinyalakan, ia belum memiliki cache ARP yang lengkap. Entri pada cache ARP yang dimilikinya hanya untuk host itu sendiri. Setelah berinteraksi dengan host lain, barulah host tersebut memiliki entri-entri tambahan pada cache ARP. Hal yang sama juga terjadi pada tabel routing di host. Pada saat host baru dinyalakan, host tersebut tidak memiliki informasi di tabel routing kecuali entri untuk jaringan lokalnya. Tabel routing seperti ini kadang-disebut sebagai tabel routing minimal. Dalam kondisi hanya memiliki tabel routing minimal, host belum siap untuk melakukan internetwork karena hanya dapat berkomunikasi dengan host-host yang terletak pada satu jaringan lokal.

Langkah pertama untuk mempersiapkan host untuk dapat melakukan fungsi internetwork adalah dengan memberikan entri rute default pada tabel routing. Dari rute default yang dimiliki pengisian tabel routing dapat dilakukan dengan beberapa metode dibawah ini :

#### **a. Routing Redirect**

Router (dalam hal ini router default) dapat menyatakan bahwa dirinya bukan rute terbaik untuk mencapai host tertentu, melainkan harus melalui router yang lain dalam jaringan lokal berdasarkan tabel routing yang dimilikinya. Jika demikian, maka router tersebut mengirimkan pesan kepada host pengirim datagram menggunakan ICMP redirect dan memberitahukan host pengirim tersebut agar datagram menuju host tertentu dialihkan

melalui router lain. Host pengirim menerima pesan ICMP redirect itu dan menambahkan entri host pada tabel routing dengan informasi routing yang baru.

### ***b. Routing Statik***

metode lain yang dapat dipakai untuk membentuk tabel routing adalah dengan memakai routing static. Pada metode ini entri-entri rute di host dan di router dimasukkan secara manual

### ***c. Protokol Routing***

protokol routing adalah protokol yang digunakan oleh router-router untuk saling bertukar informasi routing. Router-router pada jaringan TCP/IP membentuk tabel routing berdasarkan informasi routing yang dipertukarkan setiap selang waktu tertentu.

## **2.3.4 Protokol Routing**

Routing pada jaringan TCP/IP dibagi menjadi dua macam :

- ***Interior Gateway Protocol (IGP)***  
Adalah protokol routing yang menangani perutean dalam suatu sistem *autonomous*.
- ***Exterior Gateway Protocol (EGP)***  
Merupakan protokol routing yang menangani routing antar sistem *autonomous*.

Sistem *autonomous* adalah suatu sistem jaringan internet yang berada dalam satu kendali administrasi dan teknis.

Ada beberapa macam Protokol routing yang sering digunakan, diantaranya :

- ***Routing Information Protocol (RIP)***
- ***Open Shortest Path First (OSPF)***
- ***Border Gateway Protocol (BGP)***

Berdasarkan pembagian utamanya maka protokol routing yang termasuk dalam IGP adalah RIP & OSPF, sedangkan yang termasuk dalam EGP adalah BGP.

EGP memiliki kemampuan untuk menentukan policy routing karena sebagian autonomous sistem di internet mempunyai kebijakan dalam hal routing. Untuk pelaksanaan routing dalam suatu IGP policy ini tidak diperlukan.

**a. Routing Information Protocol (RIP)**

RIP memiliki karakteristik sebagai berikut :

- menggunakan algoritma distance-vektor (Bellman-Ford)
- dapat menyebabkan routing loop
- diameter jaringan terbatas
- lambat mengetahui perubahan jaringan
- menggunakan metrik tunggal

**b. Open Shortest Path First (OSPF)**

karakteristik OSPF diantaranya :

- menggunakan algoritma link-state
- membutuhkan waktu CPU dan memori yang besar
- tidak menyebabkan routing loop
- dapat membentuk hierarki routing menggunakan konsep area
- cepat mengetahui perubahan jaringan
- dapat menggunakan beberapa macam metrik

## **2.4 ADDRESS RESOLUTION PROTOCOL (ARP)**

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.

### **2.4.1 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.

### **2.4.2 Resolusi melalui Direct Mapping**

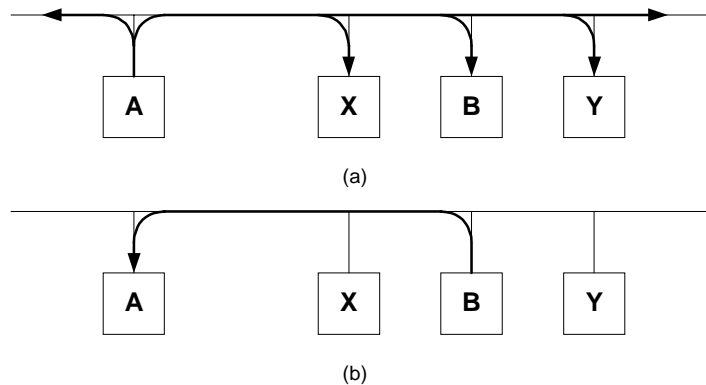
Untuk memilih skema yang membuat resolusi alamat yang efisien berarti memilih fungsi  $f$  yang memetakan alamat IP ke alamat fisik. Resolving alamat IP  $I_A$  berarti menghitung :

$$P_A = f(I_A)$$

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.

### 2.4.3 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 mmbutuhkan 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 protocol ARP

Ide dari metode ini adalah jika suatu host (A) ingin me-resolve suatu alamat ( $I_B$ ) maka A mem-broadcast paket khusus yang meminta host dengan alamat IP ( $I_B$ ) untuk meresponnya dengan alamat fisik  $P_B$ . 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 menerima reply, A menggunakan alamat tersebut untuk mengirim paket internet secara langsung ke B.

#### 2.4.4 Address Resolution Cache

Cache yang 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.

#### 2.4.5 Implementasi ARP

Secara fungsional penggunaan ARP dibagi menjadi 2 bagian :

- a. bagian penentuan alamat fisik ketika mengirimkan sebuah paket
- b. bagian penjawab suatu request dari mesin lain.

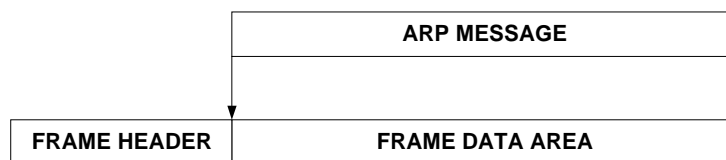
Resolusi alamat untuk paket yang dikirimkan terlihat sederhana, ttetapi memiliki implementasi yang agak kompleks.

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.

#### 2.4.6 Enkapsulasi & Identifikasi ARP

Pesan ARP terkirim dalam bentuk frame dengan format :



Gambar 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 = 0806<sub>16</sub> yang merupakan nilai standar yang digunakan di Ethernet.

### 2.4.7 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 sesuadahnya. Contoh pada gambar :

HARDWARE TYPE		HARDWARE TYPE
HLEN	PLEN	OPERATION
SENDER HA (octet 0-3)		
SENDER HA (octet 4-5)		SENDER IP (octet 0-1)
SENDER IP (octet 2-3)		TARGET HA (octet 0-1)
TARGET HA (octet 2-5)		
TARGET IP (octet 0-3)		

Gambar format pesan protokol ARP

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

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

## 2.5 INTERNET CONTROL MESSAGE PROTOCOL (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, 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 mengizinkan 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.

### **2.5.1 Error & Query Reporting**

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 & 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 logik. Pesan ini dapat dibagi menjadi beberapa tipe :

- o ***network unreachable***

jika jaringan tujuan tidak dapat dihubungi

- o ***host unreachable***

jika host tujuan tidak bisa dihubungi

- o ***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 diantaranya 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***

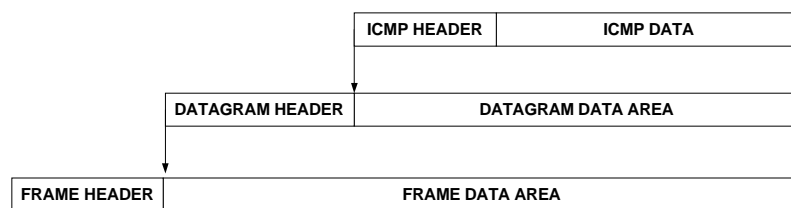
menghasilkan informasi waktu yang diperlukan sistem tujuan untuk memproses suatu paket

- ***Address Mask***

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

### **2.5.2 Pengiriman ICMP Message**

ICMP memerlukan dua level enkapsulasi seperti pada gambar dibawah ini :



Gambar Enkapsulasi pesan ICMP

Setiap pesan ICMP merupakan bagian dari datagram IP yang juga merupakan bagian 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.

### **2.5.3 Format Pesan ICMP**

Format diawali dengan 3 field :

8 bit : field TYPE yang mengidentifikasi pesan

8 bit : field CODE yang menyediakan informasi lebih jauh tentang tipe pesan

16 bit : field CHECKSUM untuk pengecekan 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 (obsolete)
16	Information Reply (obsolete)
17	Address Mask Request
18	Address Mask Reply

