BAB 2

TINJAUAN PUSTAKA

2.1 Profil Tempat Penelitian

Profil tempat penelitian yang akan dibahas pada subbab ini meliputi sejarah instansi, visi dan misi Pusair, logo instansi, badan hukum instansi, dan struktur organisasi dan deskripsi pekerjaan.

2.1.1 Sejarah Instansi

Puslitbang Sumber Daya Air merupakan salah satu dari 4 (empat) Pusat Litbang yang berada di bawah Badan Litbang Kimpraswil. Instansi ini sudah ada sejak tahun 1936 dengan nama Departement *Verheer en Waterstaat*. Pada tahun 1947 nama tersebut berubah menjadi Institute *Voor Wegen Waterboukundige Orderzoekingen* dan pada tahun 1950 berubah menjadi Institut Teknik Air dan Tanah. Pada tahun 1966 setelah nama instansi berubah menjadi Lembaga Penyelidikan Masalah Air.

Dalam sejarahnya PUSAIR melakukan perubahan nama sebanyak 9 kali, yaitu sebagai berikut :

a. Tahun 1936 : *Department voor Verkeer en Waterstaat (V en W)* mendirikan *Hidrodynamisch Laboratorium* yang menempati ruangan *Technishe Hoge School (THS)*, dengan Pimpinan Umum Prof. Ir. J. W. F. Proper. Laboratoriumnya dipimpin oleh Ir.R. Agus Prawinata. Pada tahun itu juga di komplek THS telah selesai di bangun gedung Laboratorium. Nama Laboratorium diganti menjadi *Waterloopkuding Laboratorium*,

pemimpin umumnya Prof. Ir. J. W. F. Proper dan pemimpin laboratoriumnya adalah Ir. F. Gatot.

b. Tahun 1947 : *Instituut voor Weg en Waterbouwkundige Onderzoekingen (IWWO)* yang dipimpin oleh Prof. Ir. Vluggter.
c. Tahun 1950 : Setelah penyerahan kedaulatan pimpinan dipegang oleh Ir. Soepardi dari Kementrian Pekerjaan Umum dan Perhubungan, sehingga pada tahun ini diganti lagi dengan nama Institut Teknik Air dan Tanah.
d. Tahun 1966 : Lembaga Penyelidikan Masalah Air (LPMA), di bawah Direktorat Jendral Pengairan, Departement Pekerjaan Umum dan Tenaga Listrik, dengan pimpinan pertama Ir. Rachmat Tirtotjondro.
e. Tahun 1974 : Atas dengan keputusan Presiden Republik Indonesia tentang reorganisasi Departemen Maka LPMA diubah menjadi Direktorat Penyelidikan Masalah Air (DPMA), dengan direktur utamanya masih tetap.
f. Tahun 1984 : Berdasarkan surat keputusan Presiden Republik Indonesia no.15 tahun 1984 DPMA dipindahkan dari Ditjen Pengairan ke Lingkungan Badan Litbang Departemen Pekerjaan Umum, yang baru dibentuk dengan nama baru yaitu Pusat Penelitian dan Pengembangan Pengairan.
g. Tahun 1999 : Pusat Penelitian dan Pengembangan Teknologi Sumber Daya Air, berada di bawah Litbang Departemen Pemukiman dan Pengembangan Wilayah (Kimbangwil).

h. Tahun 2001 : Pusat Penelitian dan Pengembangan Sumber Daya Air, berada di bawah Badan Litbang Departemen Pemukiman dan Prasarana Wilayah (Kimpraswil).

i. Tahun 2004 : Pusat Penelitian dan Pengembangan Sumber Daya Air (PUSAIR), berada di bawah Badan Litbang Departemen Pekerjaan Umum.

2.1.2 Visi dan Misi Pusair

1. Visi

   Terwujudnya Ilmu Pengetahuan dan Teknologi (IPTEK) Sumber Daya Air (SDA) yang aplikatif, inovatif dan kompetitif untuk meningkatkan efisiensi dan kualitas pembangunan pemukiman dan prasarana wilayah (Kimpraswil).

   Menjadi lembaga terkemuka dalam menyediakan jasa keahlian teknologi untuk mendukung tersedianya infrastruktur Sumber Daya Air (SDA) yang handal.

2. Misi

   a. Menciptakan iklim litbang yang kondusif.

   b. Meneliti dan mengembangkan teknologi tepat guna bidang Sumber Daya Air (SDA) yang kompetitif dan ramah lingkungan.

   c. Menciptakan produk Litbang yang aplikatif dan inovatif.

   d. Menyusun norma, standar, pedoman, manual bidang kontruksi dan bangunan Sumber Daya Air.

   e. Membina hubungan kerjasama IPTEK Sumber Daya Air.

   f. Mengkaji dan mengevaluasi produk IPTEK Sumber Daya Air.

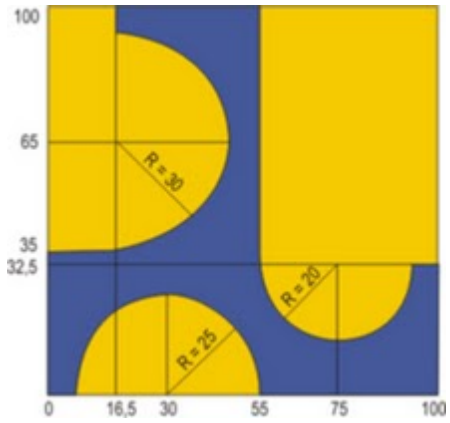
g. Mensosialisasikan IPTEK Litbang.

h. Melakukan pelayanan kegiatan Litbang pada Masyarakat.

i. Menyediakan data dan informasi bidang Sumber Daya Air (SDA).

2.1.3 Logo Instansi

LAMBANG DEPARTEMEN PEKERJAAN UMUM



Gambar 2.1 Logo Departemen Pekerjaan Umum

Keterangan :

a. Lambang Departemen Pekerjaan Umum berlukiskan Baling-baling dengan ketentuan seperti tercantum pada gambar

b. Warna dasar lambang adalah kuning (kuning kunyit).

c. Warna baling-baling adalah biru kehitam-hitaman.

d. Penggunaan lambang : lihat Manual Tata Persuratan.

ARTI SIMBOLIS LAMBANG DEPARTEMEN PEKERJAAN UMUM

1. Baling-baling
    a. Menggambarkan “Dinamika”,
    b. Berdaun 3 yang merupakan segitiga berdiri tegak lurus menggambarkan “Stabilitas Yang Dinamis”.
    c. Secara keseluruhan menggambarkan “Dinamika Yang Stabil” dan “Stabilitas Yang Dinamis”.
2. Bagian daun baling-baling yang mengarah keatas. Melambangkan “Penciptaan ruang”.
3. Bagian lengkungnya dari daun baling-baling. Memberikan perlindungan untuk ruang kerja tempat tinggal bagi manusia.
4. Bagian daun baling-baling yang mengarah ke kiri dengan bagian lengkungnya yang telungkup.
    a. Menggambarkan penguasaan bumi di alam dan pengusahaan untuk sebesar-besarnya kemakmuran rakyat.
    b. Garis horizontal : bentang jalan / jembatan diatas sungai sebagai usaha untuk pembukaan dan pembinaan daerah.
5. Bagian daun baling-baling yang mengarah ke kanan dengan bagian lengkungnya yang terlentang.
    a. Menggambarkan usaha pengendalian dan penyaluran untuk dimanfaatkan bagi sebesar-besarnya kemakmuran rakyat.
    b. Garis horizontal : bentang jalan / jembatan diatas sungai sebagai usaha untuk pembukaan dan pembinaan daerah.

6. Baling-baling dengan 3 daun ini menggambarkan :
    a. Tiga unsur kekaryaan Departemen Pekerjaan Umum. Tirta, Wisma (Cipta) dan Marga.
    b. Trilogi Departemen Pekerjaan Umum, Bekerja keras, Bergerak Cepat, Bertindak tepat.
7. Warna
    a. Warna kuning sebagai warna dasar melambangkan keagungan yang mengandung arti KeTuhanan Yang Maha Esa, Kedewasaan dan Kemakmuran.
    b. Warna biru kehitam-hitaman, mengandung arti Keadilan Sosial, Keteguhan Hari, Kesetiaan pada tugas dan ketegasan bertindak.
8. Lambang P.U

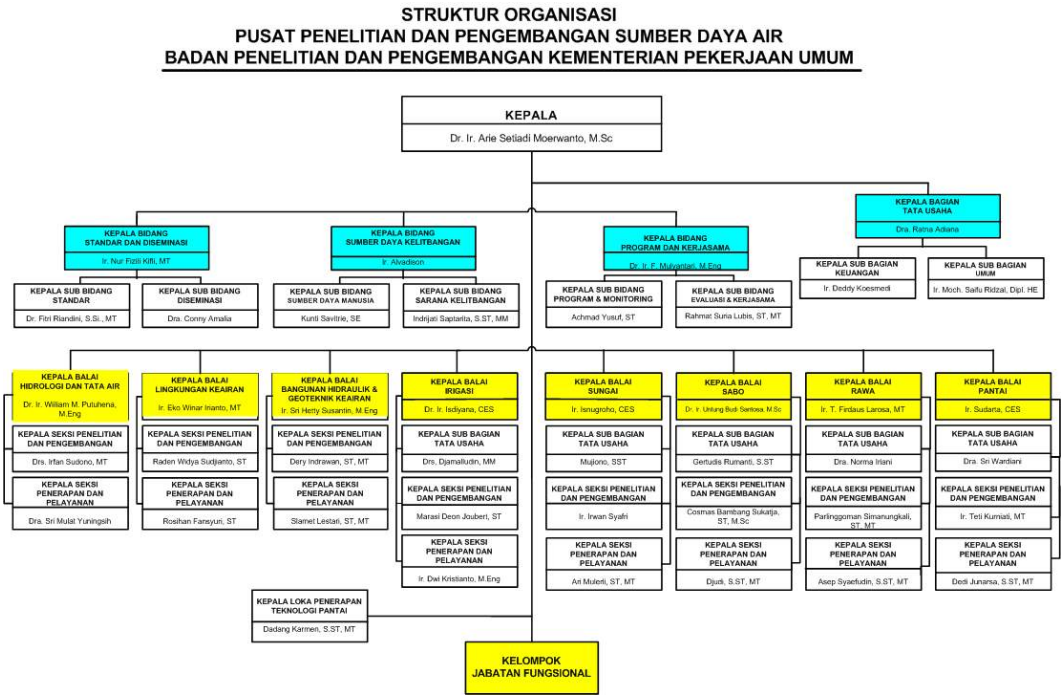
    Menggambarkan fungsi dan peranan Departemen Pekerjaan Umum dalam Pembangunan dan Pembinaan prasarana guna memanfaatkan bumi dan air serta kekayaan alam bagi kemakmuran rakyat, berlandaskan Pancasila.

2.1.4 Badan Hukum Instansi

Sebagaimana tercantum dalam Peraturan Menteri Pekerjaan Umum Nomor : 286/PRT/M/2005 Tentang Organisasi dan Tata Kerja Departemen Pekerjaan Umum, menurut Pasal 915 sampai 921.[1]

2.1.5 Struktur Organisasi dan Deskripsi Pekerjaan

2.1.5.1 Struktur Organisasi Pusair



Gambar 2.2 Struktur Organisasi PUSAIR

2.1.5.2 Deskripsi Pekerjaan

a. Bagian Tata Usaha

Bagian tata usaha mempunyai tugas melaksanakan urusan administrasi perkantoran, keuangan dan pembendaharaan. Dalam melaksanakan tugasnya bagian tata usaha memiliki fungsi :

1) Pelaksanaan urusan perbendaharaan, pelaksanaan anggaran dan pengelolaan PNBP (penerimaan Negara Bukan Pajak), serta verifikasi dan akuntansi keuangan.

2) Pelaksanaan urusan administrasi perkantoran dan penyelenggaraan rumah tangga.

Sub bagian Tata Usaha terdiri dari :

a) Sub Bagian Keuangan

Sub bagian keuangan mempunyai tugas melakukan penerapan peraturan perbendaharaan, pengelolaan anggaran keuangan dan pelaksanaan pembiayaan, verifikasi dan akuntansi termasuk kegiatan PNBP (Penerimaan Negara Bukan Pajak).

b) Sub Bagian Tata Usaha

Sub bagian tata usaha dan rumah tangga mempunyai tugas melakukan urusan tata usaha perkantoran, IKMN (Inventarisasi Kelompok Milik Negara), pemeliharaan gedung dan rumah tangga.

b. Bagian pengembangan keahlian dan sarana kelitbangan

Bidang pengembangan keahlian dan sarana kelitbangan mempunyai tugas melaksanakan perencanaan dan pengembangan keahlian, pengelolaan jabatan fungsional dan sumber daya manusia litbang serta pengembangan sarana kelitbangan. Dalam melaksanakan tugas, Bidang Pengembangan Keahlian dan Sarana Kelitbangan memiliki fungsi :

1) Pelaksanaan urusan pengembangan keahlian, fasilitas HaKi, pengelolaan organisasi dan tata laksana dan pengembangan jabatan fungsional serta pengelolaan SDM litbang.

2) Pengembangan sarana Litbang dan Laboratorium pengujian serta pengurusan sertifikasi dan akreditasi.

Bidang Pengembangan Keahlian dan Sarana Kelitbangan terdiri dari:

a) Sub Bidang Pengembangan Keahlian

Sub bidang pengembangan keahlian mempunyai tugas melakukan perencanaan program, kebutuhan pendidikan dan kebutuhan jabatan fungsional, monitoring dan evaluasi perkembangan jabatan fungsional, fasilitas pengajuan angka kredit, organisasi dan tata laksana, serta membantu pengelolaan Sumber Daya Air.

b) Sub Bidang Pengembangan Sarana

Sub bidang pengembangan sarana mempunyai tugas melakukan perencanaan, pengembangan sarana litbang, serta pengurusan akreditasi laboratorium.

c. Bidang Standard dan Diseminasi

Bidang standard dan diseminasi mempunyai tugas mengkoordinasikan perumusan standar, fasilitas dan evaluasi penerapan standar, melaksanakan diseminasi dan informasi serta pelayanan advis teknis bidang sumber daya air. Dalam melaksanakan tugas Bidang Standard dan Diseminasi Menyelenggarakan fungsi :

1) Koordinasi perumusan bahan standard dan manual iptek, serta fasilitas penerapan dan kaji ulang standar.

2) Penyebaruasan dan pelayanan data dan informasi hasil litbang, pengelolaan dokumentasi dan perpustakaan, serta koordinasi pelayanan advis teknis bidang sumber daya air.

Bidang Standard dan Diseminasi terdiri dari :

a) Sub Bidang Standar

Sub bidang standar mempunyai tugas pengumpulan data, perumusan, kordinasi penyusunan, monitoring dan evaluasi penerapan, preview dan revisi standar bidang sumber daya air.

b) Sub Bidang Diseminasi

Sub Bidang diseminasi mempunyai tugas melaksankan dokumentasi dan perpustakaan, publikasi dan fasilitasi penyebarluasan hasil litbang dan standar, kordinasi layanan advis teknis bidang sumber daya air.

d. Bidang Program dan Kerjasama

Bidang program dan kerja sama mempunyai tugas menyusun RENSTRA (Rencana Strategic) dan program tahunan, monitoring dan evaluasi serta pengembangan kerjasama dan kemitraan hasil litbang bidang sumber daya air.

Dalam melaksankan tugas, Bidang Program dan Kerjasama menyelenggarakan fungsi :

1) Penyusunan rencana strategis dan program tahunan, monitoring dan evaluasi kegiatan litbang sumber daya air.
2) Pengembangan kerjasama litbang dalam dan luar negri serta mengkoordinasikan kemitraan hasil litbang sumber daya air dengan stakeholder terkait.

Bidang Program dan Kerjasama terdiri dari :

a) Sub Bidang Program dan Evaluasi

Sub bidang program dan evaluasi mempunyai tugas melakukan penyusunan rencana stratejik penyelenggaraan litbang, penyusunan program dan anggaran litbang tahunan, pemantauan pelaksanaan litbang, evaluasi dan pelaporan kinerja hasil litbang.

b) Sub Bidang Pengembangan Kerjasama

Sub bidang pengembangan kerjasama mempunyai tugas melakukan kerjasama dalam dan luar negri untuk menyelenggarakan litbang, kehumasan, pengurusan administrasi dan anggaran kerjasama kemitraan, korporasi dan koordinasi dalam pelaksanaan.

e. Kelompok Jabatan Fungsional

Kelompok jabatan fungsional peneliti dan jabatan fungsional sesuai dengan bidang keahliannya, yang dipimpin oleh tenaga fungsional senior yang ditujuk oleh Kepala Pusat Litbang Pengairan.

Serta adapun Balai di lingkungan Pusat Penelitian dan Pengembangan Puslitbang Sumber Daya Air :

1) Balai Lingkungan Keairan

Lingkungan kegiatan Litbang meliputi kualitas air (kimia, fisika, biologi, dan sendiment suspensi) baku mutu lingkungan keairan, pencemaran air, pengolahan dan pengelolaan air limbah, daya dukung sumber air, instrumentasi pemantauan kualitas air dan lain-lain. Aktivitas pembangunan pengelolaan dan pemanfaatan Sumber Daya Air di upayakan untuk tidak berdampak negatif terhadap lingkungan, sumber-sumber air dapat dimanfaatkan.

2) Balai Hidrologi

Cakupan kegiatan Litbang meliputi banjir, kekeringan, erosi-sendimentasi, hujan-aliran, air-tanah, instrumentasi hidrologi, klimatologi dan lain-lain. Inovasi dan perekayasaan teknologi ini dapat mendukung pembangunan prasarana Sumber Daya Air seperti untuk pengendalian sungai, pembangunan bendung dan bendungan, pengendalian bencana alam dan sebagainya.

3) Balai Hidraulik

Cakupan kegiatan Litbang meliputi permasalahan aliran (debit, kecepatan, aliran, tinggi muka air), energi hidraulik (pemanfaatan energi, pemecahan energi), instrumentasi hidraulika sangat berperan untuk mempelajari kinerja saluran, sungai, pantai, aliran dalam pipa, turbin dan hidraulika lainnya.

4) Balai Geoteknik

Cakupan kegiatan Litbang meliputi permasalahan bahan bangunan seperti tanah dan bebatuan, stabilitas lereng dan bangunan, galian dan timbunan, permeabilitas porositas tanah, kegempaan. Instrumentasi geoteknik, daya dukung tanah dan batuan dan lainnya. Prasarana Sumber Daya Air yang berupa bangunan yang harus dapat berdiri dengan stabil, dibuat dari bahan yang berkualitas tinggi, mempunyai kedapan sesuai dengan yang diisyaratkan. Untuk hal itu, maka penyelidikan tentang geoteknik sangat berperan.

5) Balai Sungai

Litbang sungai diarahkan pada fenomena morfologi sungai, agradasi dan degradasi sungai. Sungai yang merupakan prasaran Sumber Da Air akan dapat dikelola dan dimanfaatkan seoptimal mungkin serta dapat dikendalikan agar dampak negative yang timbul dapat ditekan menjadi sekecil mungkin.

6) Balai Sabo

Cakupan kegiatan Libtang meliputi pencegahan kerusakan sungai akibat muntahan dari letusan gunung berapi yang dikenal dengan debris, lahan dan daerah yang rawan aliran sendimen. Teknologi sabo sangat berperan untuk melindungi penduduk, harta benda, lahan pertanian, bangunan prasarana Sumber Daya Air dan jalan.

7) Balai Rawa dan Pantai

Kegiatan litbang mencakup fenomena pasang surut, tanah lunak, gelombang dan perendaman energi, erosi abrasi, penyumbatan muara, drainase, reklamasi dan tambak. Daerah rawa yang digunakan untuk budidaya pertanian dan pertambakan akan dapat ditingkatkan fungsi dan pemanfaatannya. Daerah pantai dapat dikembangkan sesuai dengan peruntukannya dan gejala kerusakan pantai akan dapat dikendalikan dan dilindungi sehingga menjadi daerah produktif dan aman.

8) Balai Irigasi

Lingkup kegiatan litbang berkaitan dengan efisiensi penggunaan air irigasi, keakuratan perhitungan kebutuhan air irigasi, pengendalian kebocoran dan kehilangan air (peresapan, penguapan, kelebihan), pemilihan pola tanam, sistem pemberian air, bangunan-bangunan prasarana dan sarana irigasi, instrumentasi dan sebagainya.

2.2 Landasan Teori

Pada subbab ini, akan dibahas beberapa landasan teori antara lain jaringan komputer, topologi jaringan, *transmission control protocol / internet protocol (tcp/ip),* komunikasi tcp/ip, *protocol*, istilah-istilah dalam *internet protocol*, prinsip kerja *internet protocol*, prinsip kerja *transmission control protocol*, *internet protocol version 4 (IPv4),* dan *internet protocol version 6 (IPv6).*

2.2.1 Jaringan Komputer

Jaringan komputer adalah sekelompok komputer otonom yang dihubungkan satu dengan yang lainnya dengan menggunakan protokol komunikasi melalui media transmisi atau media komunikasi sehingga dapat saling berbagi data informasi, program–program, *share* perangkat keras seperti *printer* atau *harddisk*. Tujuan dibangunnya suatu jaringan komputer adalah untuk membawa data informasi dari sisi pengirim menuju penerima secara cepat dan tepat tanpa adanya kesalahan melalui media transmisi atau media komunikasi tertentu.

2.2.1.1 Jenis Jaringan Komputer

Jaringan komputer yang digunakan saat ini dapat dikelompokkan berdasarkan area yang dapat dijangkau. Area ini mulanya ditentukan berdasarkan jarak jangkau dalam satuan meter. Namun dalam perkembangan selanjutnya berdasarkan peralatan dan fasilitas. Penggunaan peralatan–peralatan yang dimaksud adalah peralatan–peralatan *internet* jaringan seperti *repeater*, *router* atau *gateway* dari peralatan tersebut dapat dilihat jangkauan area jaringan dan luasan segmen jaringan yang dibangun.

Berdasarkan kriteria–kriteria tersebut secara umum jaringan komputer dapat digolongkan sebagai Berikut ini merupakan :

1. *Local Area Network (LAN)*
2. *Metropolitan Area Network (MAN)*
3. *Wide Area Network (WAN)*
4. *Wireless Network*

a. *Local Area Network* (LAN)

Sebuah LAN adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan seperti sebuah perkantoran di sebuah gedung, atau sebuah sekolah, dan biasanya sekitar 1 km persegi.. Komputer-komputer yang terhubung ke dalam jaringan itu biasanya disebut dengan *workstation.* Kebanyakan LAN menggunakan media kabel untuk menghubungkan antara satu komputer dengan komputer lainnya.

b. *Metropolitan Area Network* (MAN)

Sebuah MAN, biasanya meliputi area yang lebih besar dari LAN, misalnya antar wilayah dalam satu provinsi. Dalam hal ini jaringan menghubungkan beberapa buah jaringan-jaringan kecil ke dalam lingkungan area yang lebih besar.

c. *Wide Area Network* (WAN)

Wide Area Networks (WAN) adalah jaringan yang lingkupnya biasanya sudah menggunakan sarana satelit ataupun kabel bawah laut sebagai contoh keseluruhan jaringan suatu Bank yang ada di Indonesia ataupun yang ada di negara - negara lain. menggunakan sarana WAN, Sebuah Bank yang ada di Bandung bisa menghubungi kantor cabangnya yang ada di Jepang, hanya dalam

beberapa menit. Biasanya WAN agak rumit dan sangat kompleks, menggunakan banyak sarana untuk menghubungkan antara LAN dan WAN ke dalam komunikasi global seperti Internet. Tapi bagaimanapun juga antara LAN, MAN dan WAN tidak banyak berbeda dalam beberapa hal, hanya lingkup areanya saja yang berbeda satu diantara yang lainnya.

d. *Wireless Network*

Wireless Network merupakan peralatan *end-user* untuk megakses jaringan dengan menggunakan transmisi radio pendek atau sedang.

Wireless WAN : GSM (sampai 20 Kbps)

Wireless LAN/MAN : WaveLAN (2-11 Mbps, sampai 150 m)

Wireless PAN (*Personal Area Network*) : *Bluetooth (*sampai 2 Mbps, jarak < 10 m*)*

Tabel 2.1 Susunan Jaringan Komputer menurut Jarak

	Range	***Bandwidth* (Mbps)**	**Latency (ms)**
LAN	1-2 kms	10-1000	1-10 ms
WAN	*Worldwide*	0.010-600	100-50 ms
MAN	2-50 kms	1-150	10 ms
Wireless LAN	0.15-1.5 km	2-11	5-20 ms
Wireless WAN	*Worldwide*	0.010-2	100-500 ms
Internet	*Worldwide*	0.010-2	100-500

2.2.1.2 Tipe Jaringan

Dalam jaringan komputer terdapat dua tipe jaringan, yaitu :

1. Model *client-server.*
2. Model *peer to peer* atau *point to point.*

a. Jaringan *Client-Server*

Konsep Jaringan *client-server* ini membedakan dengan jelas kedudukan suatu komputer, mana yang dapat memberikan layanan jaringan (*server*) dan mana yang hanya meminta layanan (*client*). Jika suatu komputer di*install* sebagai *server* yang memberikan segala sumber daya (*resource*), contohnya : *printer*, *modem* kepada komputer lain (*client)* yang terhubung ke jaringan. Untuk dapat saling berkomunikasi antara *server* dan *client*, maka digunakan suatu aplikasi jaringan yang dinamakan *client-server program*, dimana *server* menggunakan aplikasi jaringan yang disebut *server program*, sementara *client* menggunakan *client program* untuk dapat berkomunikasi dengan *server program* pada *server*.

Beberapa sifat dari *client-server* diantaranya sebagai Berikut ini merupakan :

a. *Server* dan *Client* berada pada posisi serta proses yang berbeda.
b. *Server* dan *Client* dapat dijalankan pada mesin yang sama atau berbeda.
c. Setiap proses dapat menyembunyikan informasi tersendiri.
d. Komunikasi yang dilakukan bisa bersifat protokol *peer to peer*.

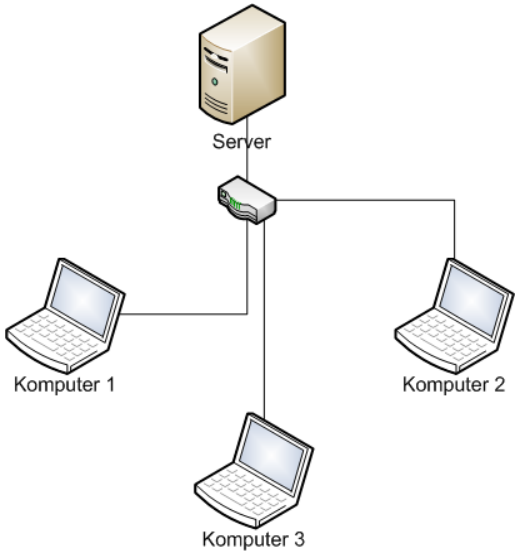
Konektivitas *client ke Server :*

a. *Server* harus terlebih dahulu dijalankan (*running*).

b. *Server* harus menentukan *port* untuk koneksi yang masuk.

c. *Client* harus mengetahui nama *Host* dari *server* beserta *port* yang digunakan untuk koneksi.

d. *Client* mengirim pesan ke *server* untuk melakukan suatu pekerjaan (*task*). *Server* dan *Client* bersifat *Asimetrik.*



Gambar 2.3 Jaringan *Client-Server*

Berikut ini merupakan kelebihan dan kekurangan dari jaringan *client-server.*

Tabel 2.2 Keunggulan dan Kelemahan *Client-Server*

KEUNGGULAN	KELEMAHAN
Kecepatan akses lebih tinggi karena penyediaan fasilitas jaringan dan pengelolaannya dilakukan secara khusus oleh satu komputer (*server*) yang tidak dibebani dengan tugas lain sebagai *workstation*.	Biaya operasional relatif lebih mahal.

Sistem keamanan dan administrasi jaringan lebih baik, karena terdapat seorang pemakai yang bertugas sebagai administrator jaringan, yang mengelola administrasi dan sistem keamanan jaringan.	Diperlukan adanya satu komputer khusus yang berkemampuan lebih untuk ditugaskan sebagai *server*.
Sistem *backup* data lebih baik, karena pada jaringan *client-server backup* dilakukan terpusat di *server*, yang akan membackup seluruh data yang digunakan di dalam jaringan.	Kelangsungan jaringan sangat tergantung pada *server*. Bila *server* mengalami gangguan maka secara keseluruhan jaringan akan terganggu.

b. Jaringan *Peer to peer*

Pada model jaringan terdapat hanya dua komputer yang saling terhubung. Masing-masing komputer mempunyai kedudukan yang setara atau setingkat sehingga komputer manapun dapat memulai (*initiate*) dan mengendalikan hubungan dalam jaringan. Model Jaringan ini merupakan jenis yang paling sederhana.



Gambar 2.4 Jaringan *Peer to Peer*

Berikut ini merupakan kelebihan dan kekurangan dari jaringan *peer to peer*.

Tabel 2.3 Keunggulan dan Kelemahan *peer to peer*

KEUNGGULAN	KELEMAHAN
Antar komputer dalam jaringan dapat saling berbagi-pakai fasilitas yang dimilikinya seperti *harddisk, drive, fax/modem, printer*.	*Troubleshooting* jaringan relatif lebih sulit, karena pada jaringan tipe *peer to peer* setiap komputer dimungkinkan untuk terlibat dalam komunikasi yang ada. Di jaringan *client-server*, komunikasi adalah antara *server* dengan *workstation*.
Biaya operasional relatif lebih murah dibandingkan dengan tipe jaringan *client-server*, salah satunya karena tidak memerlukan adanya *server* yang memiliki kemampuan khusus untuk mengorganisasikan dan menyediakan fasilitas jaringan.	Unjuk kerja lebih rendah dibandingkan dengan jaringan *client-server*, karena setiap komputer disamping harus mengelola pemakaian fasilitas jaringan juga harus mengelola pekerjaan atau aplikasi sendiri.
Kelangsungan kerja jaringan tidak tergantung pada satu *server*. Sehingga bila salah satu komputer/peer mati atau rusak, jaringan secara keseluruhan tidak akan mengalami gangguan.	Sistem keamanan jaringan ditentukan oleh masing-masing user dengan mengatur keamanan masing-masing fasilitas yang dimiliki.

2.2.2 Topologi Jaringan

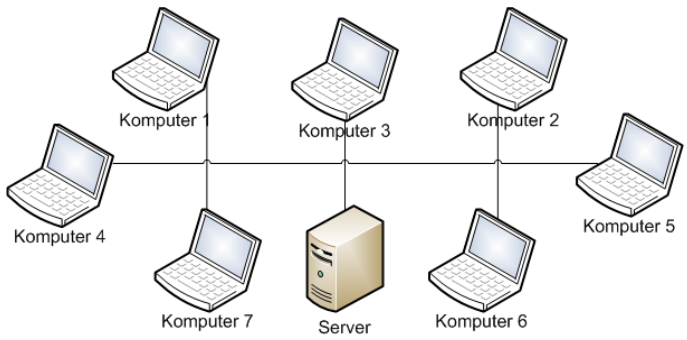
Topologi jaringan merupakan suatu struktur atau bagaimana menghubungkan antara simpul dan pusat dalam suatu jaringan. Tiap struktur mempunyai keuntungan dan kerugiannya masing-masing.

Bentuk-bentuk arsitektur jaringan komputer secara fisik adalah sebagai Berikut ini merupakan

1. Topologi *Bus.*
2. Topologi *Star.*
3. Topolgi *Tree.*
4. Topologi *Ring.*

2.2.2.1 Topologi *Bus*

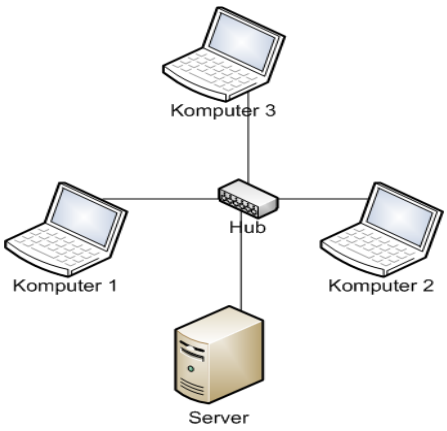
Topologi sebuah bus merupakan garis lurus yang terdiri dari satu jalur kabel utama (*backbone*) dimana pada masing-masing ujungnya diberikan sebuah *terminator*. Semua *nodes* pada jaringan (*file server, workstation,* dan perangkat lainnya) terkoneksi ke sebuah kabel utama. Jaringan-jaringan *Ethernet* dan *Localtalk* menggunakan topologi *linear* ini.



Gambar 2.5 Topologi *Bus*

2.2.2.2 Topologi *Star*

Topologi model ini didesain dimana setap *node* (*file server*, *workstation*, dan perangkat lainnya) terkoneksi ke jaringan melewati sebuah *concentrator* baik berupa *HUB* ataupun *SWITCH*. Data yang terkirim ke jaringan akan melewati *concentrator* sebelum melanjutkan ke tempat tujuannya. *Concentrator* akan mengatur dan mengontrol keseluruhan fungsi jaringan. Dia juga bertindak sebagai *repeater* dalam skala kecil dari aliran data. Konfigurasi pada jaringan model ini menggunakan kabel *Twisted Pair*.

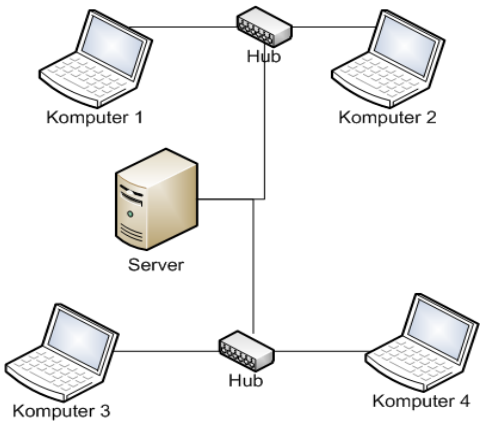


Gambar 2.6 Topologi star

2.2.2.3 Topologi *Tree*

Sebuah topologi model ini merupakan perpaduan antara topologi *Linear BUS* / Garis Lurus dan Bintang, yang terdiri dari kelompok-kelompok dari *workstation* konfigurasi Bintang yang terkoneksi ke kabel utama yang menggunakan topologi *Linear BUS* / Garis Lurus. Topologi ini memungkinkan untuk pengembangan jaringan yang telah ada, dan memungkinkan sebuah perusahaan mengkonfigurasi jaringan sesuai dengan kebutuhannya.

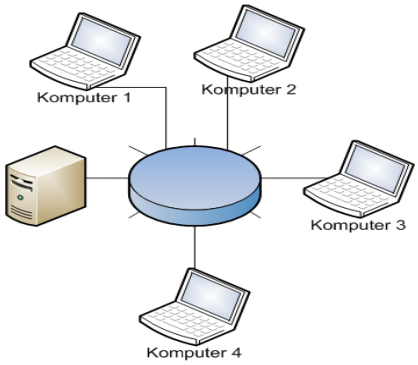
Berikut ini merupakan gambar topologi *tree*.



Gambar 2.7 Topologi *Tree*

2.2.2.4 Topologi *Ring*

Dalam topologi *Ring* semua *workstation* dan *server* dihubungkan sehingga terbentuk suatu pola lingkaran atau cincin. Tiap *workstation* ataupun *server* akan menerima dan melewatkan informasi dari satu komputer ke komputer lain, bila alamat- alamat yang dimaksud sesuai maka informasi diterima dan bila tidak informasi akan dilewatkan.



Gambar 2.8 Topologi *Ring*

2.2.3 *Transmission Control Protocol / Internet Protocol (TCP/IP)*

2.2.3.1 Sejarah TCP/IP

Internet Protocol dikembangkan pertama kali oleh *Defense Advanced Research Projects Agency* (DARPA) pada tahun 1970 sebagai awal dari usaha untuk mengembangkan protokol yang dapat melakukan interkoneksi berbagai jaringan komputer yang terpisah, yang masing-masing jaringan tersebut menggunakan teknologi yang berbeda. Protokol utama yang dihasilkan proyek ini adalah *Internet Protocol* (IP). Riset yang sama dikembangkan pula yaitu beberapa protokol level tinggi yang didesain dapat bekerja dengan IP. Yang paling penting dari proyek tersebut adalah *Transmission Control Protocol* (TCP), dan semua grup protokol diganti dengan TCP/IP *suite*. Pertama kali TCP/IP diterapkan di ARPANET, dan mulai berkembang setelah Universitas California di Berkeley mulai menggunakan TCP/IP dengan sistem operasi UNIX. Selain *Defense Advanced Research Projects Agency* (DARPA) ini yang mengembangkan *Internet Protocol*, yang juga mengembangkan TCP/IP adalah *Department of Defense* (DOD).

2.2.3.2 *Overview* TCP/IP

TCP/IP dikembangkan oleh *Department Of Defense* (DOD). DOD telah melakukan proyek penelitian untuk menghubungkan beberapa jaringan yang didesain oleh berbagai *vendor* untuk menjadi sebuah *networks of networks* (Internet). Pada awalnya hal ini berhasil karena hanya menyediakan pelayanan dasar seperti *file transfer, electronic mail, remote logon*. Beberapa komputer

dalam sebuah departemen dapat menggunakan TCP/IP (bersamaan dengan protokol lain) dalam suatu LAN tunggal. Komponen IP menyediakan *routing* dari departemen ke *network enterprise*, kemudian ke jaringan regional dan akhirnya ke global internet. Hal ini dapat menjadikan jaringan komunikasi dapat rusak, sehingga untuk mengatasinya maka kemudian DOD mendesain TCP/IP yang dapat memperbaiki dengan otomatis apabila ada *node* atau saluran telepon yang gagal. Hasil rancangan ini memungkinkan untuk membangun jaringan yang sangat besar dengan pengaturan pusat yang sedikit. Karena adanya perbaikan otomatis maka masalah dalam jaringan tidak diperiksa dan tak diperbaiki untuk waktu yang lama.

2.2.3.3 Standar TCP/IP

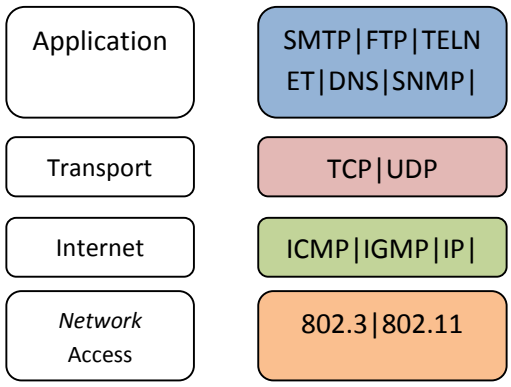
TCP/IP adalah sekumpulan protokol yang mengatur komunikasi data komputer di internet, komputer-komputer yang terhubung di internet berkomunikasi dengan protokol ini, karena menggunakan protokol yang sama maka perbedaan jenis komputer dan system operasi tidak terjadi masalah. Perkembangan protokol TCP/IP yang diterima luas dan praktis menjadi *standar de facto* jaringan komputer berkaitan denga ciri-ciri yang terdapat pada protokol itu sendiri yaitu :

1. Protokol TCP/IP dikembangkan menggunakan standar protokol terbuka (*open system*).
2. Standar protokol TCP/IP dalam bentuk *Request For Comment* (RFC) dapat digunakan oleh siapapun.

3. TCP/IP dikembangkan dengan tidak tergantung pada perangkat lunak atau perangkat keras tertentu.
4. Pengembangan TCP/IP dilakukan dengan konsensus dan tidak tergantung pada vendor tertentu.
5. TCP/IP *independent* terhadap perangkat keras, jaringan dan dapat dijalankan pada jaringan *Ethernet*, *token ring*, jalur telpon *Dial-up* dan praktis media apapun.
6. Pengalamatan TCP/IP bersifat unik dalam skala global. Dengan cara ini, komputer dapat saling terhubung walaupun jaringannya seluas internet sekarang ini.
7. TCP/IP memiliki fasilitas *routing* sehingga dapat diterapkan pada internet, dan memiliki jenis layanan lainnya.

2.2.3.4 Model TCP/IP

TCP/IP terbentuk dari empat layer (lapisan) kumpulan protokol yang bertingkat yaitu *Application layer, Transport layer, Internet layer, dan Network Access layer*.



Gambar 2.9 Model TCP/IP

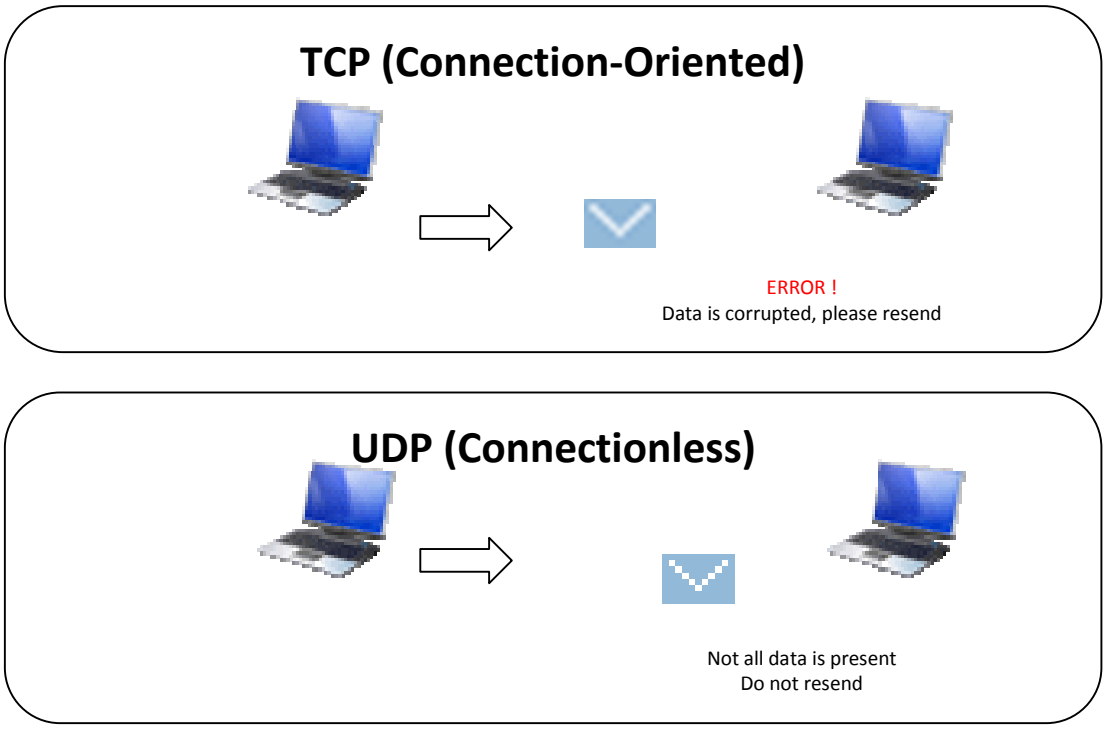
Keterangan *layer* pada TCP/IP adalah :

1. *Layer Aplikasi* adalah sebuah aplikasi yang mengirimkan data ke transport layer. Misalnya :
   a. *Domain Name Service Protocol (DNS)* digunakan untuk meresolve nama di internet menjadi alamat IP.
   b. *Hypertext Transfer Protocol (HTTP)* digunakan untuk transfer file-file halaman web di *world wide web (www).*
   c. *Telnet* merupakan suatu terminal emulator yang disediakan untuk *remote access* ke *server* atau ke perangkat jaringan lainnya.
   d. *File Transfer Portovol (FTP)* digunakan untuk mentransfer file antar system.
   e. *Simple Network Management Protocol (SNMP)* merupakan protokol standar industri yang digunakan untuk memonitor dan mengelola berbagai perangkat di jaringan internet meniputi *hub, rotuter, switch, workstation,* dan sistem manajemen jaringan secara jarak jauh (*remote*).
   f. *Simple Mail Transfer Protocol (SMTP)* digunakan untuk transfer file surat elektronik dan *attachment.*
2. *Layer Transport* bertanggung jawab untuk komunikasi antara aplikasi. Layer ini mengatur aluran informasi dan mungkin menyediakan pemeriksaan error. Data dibagi kedalam beberapa paket yang dikirim ke internet layer dengan sebuah *header*. *Header* mengandung alamat tujuan, alamat sumber dan *checksum*. *Checksum* diperiksa oleh mesin penerima untuk melihat apakah paket tersebut ada yang hilang pada rute.

Tabel 2.4 Perbedaan TCP / UDP

TCP	UDP
Reliable	Unreliable
Connection-oriented	connectionless
Segment retransmission and flow control through windowing	No windowing or retransmission
Segment sequencing	No sequencing
Acknowledge segments	No acknowledge

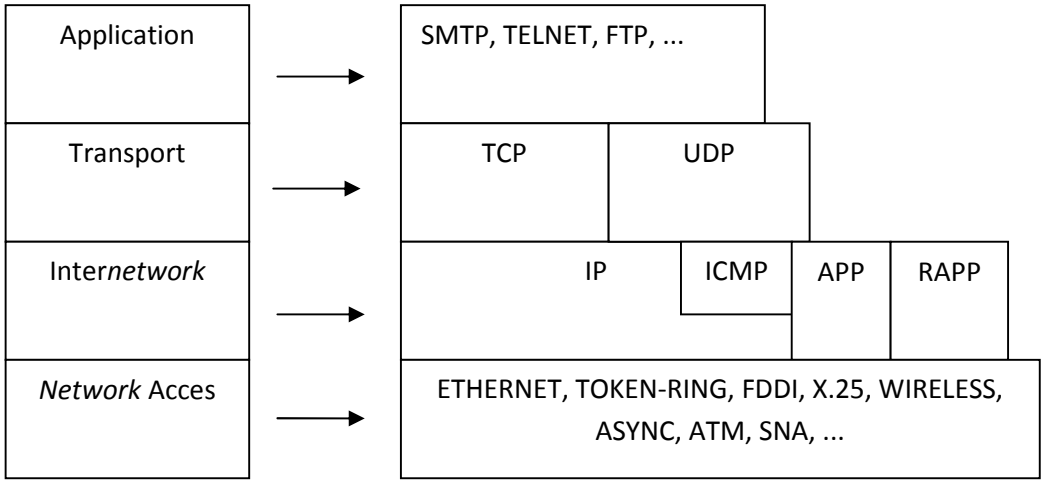
Prinsip kerja dari TCP dan UDP dapat digambarkan sebagai berikut :



Gambar 2.10 Prinsip Dasar TCP / UDP

3. *Layer Internet* bertanggung jawab untuk komunikasi antara mesin. Layer ini meg-*encapsul* paket dari transport layer ke dalam IP datagrams dan menggunakan algoritma *routing* untuk menentukan kemana datagaram harus dikirim. Masuknya datagram diproses dan diperiksa kesahannya sebelum melewatinya pada *Transport layer*.
4. *Layer Networks Access* adalah level yang paling bawah dari susunan TCP/IP. Layer ini adalah device driver yang memungkinkan datagaram IP dikirim ke atau dari fisikal *network*. Jaringan dapaat berupa sebuah kabel, *Ethernet, frame relay, Token ring, ISDN*, ATM jaringan, radio, satelit atau alat lain yang dapat mentransfer data dari sistem ke sistem. Layer *network interface* adalah abstraksi yang memudahkan komunikasi antara *multitude arsitektur network.*

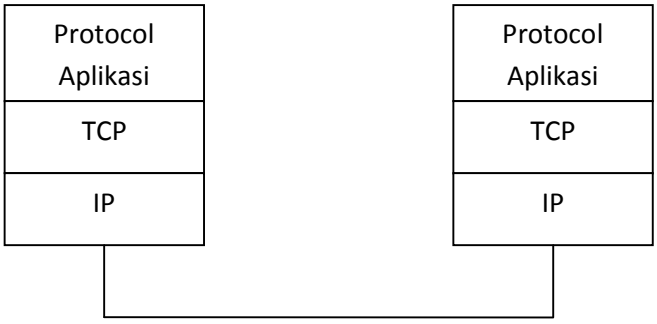
Dalam TCP/IP terjadi penyampaian data dari protokol yang berada di suatu layer ke protokol yang berada di layer lain. Jika suatu protokol menerima data dari protokol lain di layer diatasnya, protokol ini akan menambahkan informasi tambahan miliknya ke data tersebut. Informasi ini memiliki fungsi yang sesui dengan protokol tersebut. Setelah itu, data ini diteruskan lagi ke protokol pada layer dibawahnya.



Gambar 2.11 Jaringan dengan arsitektur TCP/IP

2.2.4 Komunikasi TCP/IP

Berikut ini merupakan mekanisme komunikasi antar dua komputer pada jaringan.

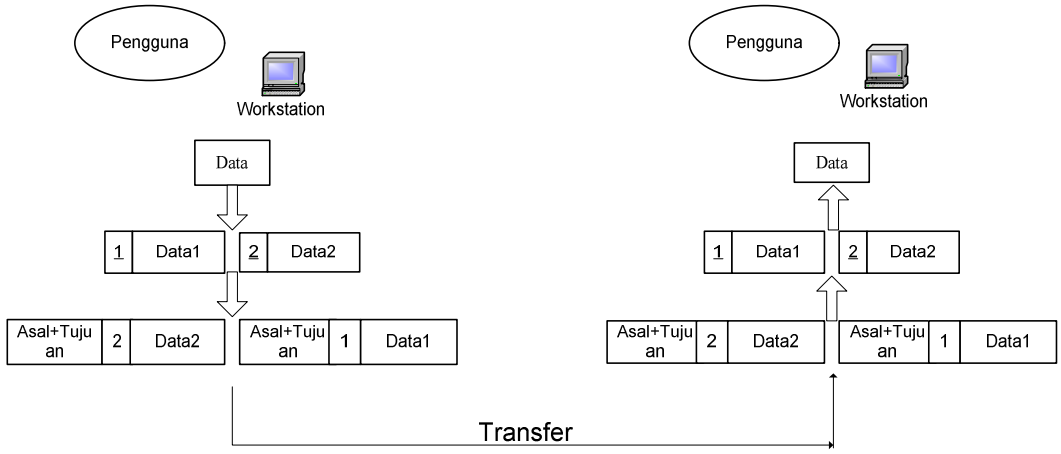


Gambar 2.12 Mekanisme Komunikasi TCP/IP

Keterangan pada gambar tersebut adalah misalkan ada dua komputer melakukan transaksi data, maka pemprosesan data yang hendak di transfer akan dilakukan oleh protokol TCP/IP. Pada komputer asal, data dari protokol aplikasi

dipecah-pecah menjadi paket-paket kemudian diberi no urut. Hal ini dilakukan pada lapisan protokol TCP, kemudian paket-paket data ini diberi keterangan berupa alamat IP komputer asal dan komputer tujuan pada lapisan protokol IP. Setelah itu paket-paket tersebut akan dikirimkan melalui media fisik.

Di komputer tujuan, lapisan IP akan melihat apakah paket-paket data yang lewat ditujukan untuk komputer tujuan atau tidak, berdasarkan alamat IP. Jika benar, paket-paket itu dikirmkan kelapisan TCP untuk diproses. Pada lapisan TCP ini, paket-paket ini dirangkai kembali sehingga dapat disajikan kepada pengguna melalui lapisan protokol aplikasi.



Gambar 2.13 Mekanisme TCP/IP

2.2.5 *Protocol*

Protokol mengatur bagaimana sebuah komputer berkomunikasi dengan komputer lain. Dalam jaringan komputer dapat digunakan bermacam-macam protokol tetapi agar ke dua buah kemputer dapat berkomunikasi keduanya perlu menggunakan protokol yang sama.

Protokol berfungsi hampir mirip bahasa, agar dapat berkomunikasi orang-orang perlu berbicara dan mengerti bahasa yang sama. Komunikasi terjadi antara berbagai entitas dengan system yang berbeda. Sebuah entitas adalah segala sesuatu yang mengirim atau menerima informasi. Bagaimanapun dua entitas tidak bisa dengan mudahnya mengirimkan Bit-bit informasi kesetiap entitas lain dan mengartikannya. Supaya komunikasi bisa terjadi, entitas harus setuju menggunakan protokol.

Protokol mengaset aturan yang mengatur komunikasi data protokol mengatur apa yang dikomunikasikan bagaimana dan kapan dikomunikasikan. Elemen penting pada protokol *Syntax, Semantics,* dan *Timing* :

1. *Syntax*, menunjukan struktur atau format dari data sebagai contoh sederhananya protokol mengharapkan delapan bit pertama dari data yaitu alamat dari pengirim, kemudian delapan bit ke dua yaitu alamat penerima dan yang terakhir sisa dari system menjadi pesan itu sendiri.
2. *Semantics*, menunjukan arti dari setiap bagian dari bit-bit.
3. *Timing*, menunjukan dua karakteristik kapan data itu seharusnya dikirim dan secepat apa data tersebut bisa dikirim.

Beberapa contoh protokol yang digunakan sesuai fungsinya, antara lain :

a. IPX/SPX : Digunakan pada Novel Netware
b. NETBIOS/NETBEUI : Digunakan pada Microsoft LAN
c. X.25/X.75/X.400 : Digunakan pada OSI/ISO
d. Apple Talk : Digunakan pada Aplle Mcintosh
e. TCP/IP-UNIX : Digunakan menjadi standar karena multiplatform komputer dan bersifat open system.

2.2.6 Istilah-istilah dalam *Internet Protocol*

Ada beberapa istilah yang sering ditemukan didalam pembicaraan mengenai TCP/IP, yaitu diantaranya :

a. *Host* atau *end-system, Host* biasanya berupa individual *workstation* atau *personal computers* (PC) dimana tugas dari *Host* ini biasanya adalah menjalankan aplikasi dan program *software server* yang berfungsi sebagai *user* dan pelaksana pelayanan jaringan komunikasi.
b. *Internet,* yaitu merupakan suatu kumpulan dari jaringan *(network of networks*) yang menyeluruh dan menggunakan protokol TCP/IP untuk berhubungan seperti *virtual networks.*
c. *Node,* adalah *i*stilah yang diterapkan untuk *router* dan *Host.protocol*, yaitu merupakan sebuah prosedur standar atau aturan untuk pendefinisian dan pengaturan transmisi data antara komputer-komputer.
d. *Router*, adalah suatu devais yang digunakan sebagai penghubung antara dua *network* atau lebih. *Router* berbeda dengan *Host* karena *router* bisanya bukan berupa tujuan atau data *traffic*. *Routing* dari datagram IP biasanya telah

dilakukan dengan software. Jadi fungsi *routing* dapat dilakukan oleh *Host* yang mempunyai dua *networks connection* atau lebih.

2.2.7 Prinsip kerja *Internet Protocol*

Fungsi dari *internet protocol* secara sederhana dapat diterangkan seperti cara kerja kantor pos pada proses pengiriman surat. Surat yang dimasukkan ke kotak pos akan diambil oleh petugas pos dan kemudian akan dikirim melalui route yang random, tanpa si pengirim maupun si penerima surat mengetahui jalur perjalanan surat tersebut. Juga jika mengirimkan dua surat yang ditujukan pada alamat yang sama pada hari yang sama, belum tentu akan sampai bersamaan karena mungkin surat yang satu akan mengambil route yang berbeda dengan surat yang lain. Di samping itu, tidak ada jaminan bahwa surat akan sampai ditangan tujuan, kecuali jika mengirimkannya menggunakan surat tercatat.

Prinsip di atas digunakan oleh *internet protocol*, "surat" diatas dikenal dengan sebutan datagram. *Internet protocol* (IP) berfungsi menyampaikan datagram dari satu komputer ke komputer lain tanpa tergantung pada media kompunikasi yang digunakan. Data *transport layer* dipotong menjadi datagram-datagram yang dapat dibawa oleh IP. Tiap datagram dilepas dalam jaringan komputer dan akan mencari sendiri secara otomatis rute yang harus ditempuh ke komputer tujuan. Hal ini dikenal sebagai transmisi *connectionless*. Dengan kata lain, komputer pengirim datagram sama sekali tidak mengetahui apakah datagram akan sampai atau tidak.

Untuk membantu mencapai komputer tujuan, setiap komputer dalam jaringan TCP/IP harus diberikan IP *address*. IP *address* harus unik untuk setiap komputer, tetapi tidak menjadi halangan bila sebuah komputer mempunyai beberapa IP *address*. IP *address* terdiri atas 8 byte data yang mempunyai nilai dari 0-255 yang sering ditulis dalam bentuk [xx.xx.xx.xx] (xx mempunyai nilai dari 0-255).

Pada *header internet protocol* selain IP *address* dari komputer tujuan dan komputer pengirim datagram juga terdapat beberapa informasi lainnya. Informasi ini mencakup jenis dari protokol *transport layer* yang ditumpangkan diatas IP. Informasi penting lainnya adalah *Time-To-Live* (TTL) yang menentukan berapa lama IP dapat hidup didalam jaringan. Nilai TTL akan dikurangi satu jika IP melalui sebuah komputer. Hal ini penting artinya terutama karena IP dilepas di jaringan komputer. Jika karena satu dan lain hal IP tidak berhasil menemukan alamat tujuan maka dengan adanya TTL IP akan mati dengan sendirinya pada saat TTL bernilai nol. Disamping itu juga tiap IP yang dikirimkan diberikan identifikasi sehingga bersama-sama dengan IP *address* komputer pengirim data dan komputer tujuan, tiap IP dalam jaringan adalah unik.

Khususnya untuk pemakai jaringan komputer hal yang terpenting untuk dipahami secara benar-benar adalah konsep IP *address*. Lembaga yang mengatur IP *address* adalah *Network* Information Center (NIC) di Department of Defence di US yang beralamat di *Host*master@nic.ddn.mil. Pengaturan IP *address* penting, terutama pada saat mengatur routing secara otomatis. Sebagai contoh jaringan komputer di amatir radio mempunyai IP *address* kelas yang mempunyai *address*

[44.xx.xx.xx]. Khusus untuk amatir radio di Indonesia IP *address* yang digunakan adalah [44.132.xx.xx]. Sedangkan penulis di Canada mempunyai IP *address* [44.135.84.22]. Hal ini terlihat dengan jelas bahwa IP *address* di amatir radio sifatnya geografis. Dari IP *address* penulis dapat dibaca bahwa mesin penulis berada di *network* 44 di InterNet yang dikenal sabagai AMPRNet (ampr.org). 135 menandakan bahwa penulis berada di Canada. 84 memberitahukan bahwa penulis berada di kota Waterloo di propinsi Ontario, sedang 22 adalah nomor mesin penulis. Dengan konsep IP *address*, route perjalanan IP dalam jaringan komputer dapat dilakukan secara otomatis. Sebagai contoh, jika sebuah komputer di InterNet akan mengirimkan IP ke [44.135.84.22], pertama-tama IP yang dilepas di *network* akan berusaha mencari jalan ke *network* 44.135.84, setelah mesin yang mengubungkan *network* 44.135.84 tercapai IP tersebut akan mencoba menghubungi mesin 22 di *network* tersebut. Kesemuanya ini dilakukan secara otomatis oleh program.

Tentunya sukar bagi manusia untuk mengingat sedemikian banyak IP *address*. Untuk memudahkan, dikembangkan *Domain Name System* (DNS). Sebagai contoh mesin penulis di AMPRNet dengan IP *address* [44.135.84.22], penulis beri nama (*Hostname*) ve3.yc1dav.ampr.org. Terlihat bahwa *Hostname* yang digunakan penulis sangat spesifik dan sangat memudahkan untuk mengetahui bahwa penulis berada di AMPRNet dari kata ampr.org. Mesin tersebut berada di Kanada dan propinsi Ontario dari ve3 sedang yc1dav adalah penulis sendiri. Contoh lain dari DNS adalah sun1.vlsi.waterloo.edu yang merupakan sebuah Sun SPARC *workstation* (sun1) di kelompok peneliti VLSI di

University of Waterloo, Kanada (waterloo.edu) tempat penulis bekerja dan belajar. Perlu dicatat bahwa saat ini NIC belum memberikan domain untuk Indonesia. Mudah-mudahan dengan berkembangnya jaringan komputer TCP/IP di Indonesia ada saatnya dimana di Indonesia perlu meminta domain tersendiri untuk Indonesia.

2.2.8 Prinsip Kerja *Trasnmission Control Protocol*

Berbeda dengan *internet protocol* (IP), TCP mempunyai prinsip kerja seperti *virtual circui*" pada jaringan telepon. TCP lebih mementingkan tata-cara dan keandalan dalam pengiriman data antara dua komputer dalam jaringan. TCP tidak perduli dengan apa-apa yang dikerjakan oleh IP, yang penting adalah hubungan komunikasi antara dua komputer berjalan dengan baik. Dalam hal ini, TCP mengatur bagaimana cara membuka hubungan komunikasi, jenis aplikasi apa yang akan dilakukan dalam komunikasi tersebut (misalnya mengirim e-mail, transfer file dsb.) Di samping itu, juga mendeteksi dan mengoreksi jika ada kesalahan data. TCP mengatur seluruh proses koneksi antara satu komputer dengan komputer yang lain dalam sebuah jaringan komputer. Mekanisme *connectionless* pada TCP mekanisme hubungan adalah *connection oriented*. Dalam hal ini, hubungan secara logik akan dibangun oleh TCP antara satu komputer dengan komputer yang lain. Dalam waktu yang ditentukan komputer yang sedang berhubungan harus mengirimkan data atau *acknowledge* agar hubungan tetap berlangsung. Jika hal ini tidak sanggup dilakukan maka dapat

diasumsikan bahwa komputer yang sedang berhubungan, mengalami gangguan dan hubungan secara logik dapat diputus.

TCP mengatur *multiplexing* dari data yang dikirim/diterima oleh sebuah komputer. Adanya identifikasi pada TCP *header* memungkinkan *multiplexing* dilakukan. Hal ini memungkinkan sebuah komputer melakukan beberapa hubungan TCP secara logik. Bentuk hubungan adalah *full duplex*, hal ini memungkinkan dua buah komputer saling berbicara dalam waktu bersamaan tanpa harus bergantian menggunakan kanal komunikasi. Untuk mengatasi saturasi (*congestion*) pada kanal komunikasi, pada *header* TCP dilengkapi informasi tentang *flow control*.

Hal yang cukup penting untuk dipahami pada TCP adalah *port number*. *Port number* menentukan servis yang dilakukan oleh program aplikasi diatas TCP. Nomor-nomor ini telah ditentukan oleh *Network Information Center* dalam *Request For Comment* (RFC) 1010 [10]. Sebagai contoh untuk aplikasi *File Transfer Protokol* (FTP) diatas *transport layer* TCP digunakan port number 20 dan masih banyak lagi.

Prinsip kerja dari TCP berdasarkan prinsip *client-server*. *Server* adalah program pada komputer yang secara pasif akan mendengarkan (*listen*) *port number* yang telah ditentukan pada TCP. Sedang *client* adalah program yang secara aktif akan membuka hubungan TCP ke komputer *server* untuk meminta servis yang dibutuhkan.

Client akan secara aktif membuka hubungan (*active open*) dengan mengirimkan sinyal SYN (state SYN SENT) ke komputer *server* tujuan. Jika

server menerima sinyal SYN maka *server* yang saat itu berada pada state LISTEN akan mengirimkan sinyal SYN dan ke dua komputer (*client* & *server*) akan ke state ESTAB. Jika tidak ada tanggapan dari komputer yang dituju, maka program akan kembali pada state CLOSE. Setelah servis yang dilakukan telah selesai maka salah *client* akan mengirimkan sinyal FIN dan komputer *client* akan berada pada state FIN WAIT sampai sinyal FIN dari *server* diterima. Pada saat menerima sinyal FIN, *server* akan ke state CLOSE WAIT hingga hubungan diputus. Akhirnya kedua komputer akan kembali pada state CLOSE.

2.2.9 *Internet Protocol version 4 (IPv4)*

Alamat *network* memberikan identifikasi unik setiap jaringan komputer. Setiap *device* pada jaringan komputer yang sama menggunakan alamat *network* yang sama. Pada IP 192.168.252.13, sebagai contoh, yang menjadi alamat *network* adalah angka 192.168.

Alamat node memberikan identifikasi secara unik pada setiap mesin di dalam suatu jaringan komputer. Bagian dari alamat ini harus unik, karena hanya mengidentifikasikan satu device dan bukan satu grup seperti alamat *network*. Alamat ini juga sering disebut dengan alamat *Host*. Pada IP 192.168.252.13, sebagai contoh yang menjadi alamat *Host* adalah 252.l13.

Alamat IPv4 dibagi menjadi 3 jenis yaitu :

1. Alamat *Unycast*

   Alamat ini digunakan dalam komunikasi *point to point.*

2. Alamat *Broadcast*

   Alamat ini digunakan dalam komunikasi *one to everyone.* Biasanya dipakai dalam satu segmen jaringan yang sama.

3. Alamat *Multicast*

   Alamat ini digunakan dalam komunikasi *one to many.*

IPv4 mengenal dua macam IP *address* yaitu IP *Public* dan IP *Private*.

a. IP *Public*

   IP *Public* adalah IP *address* yang digunakan untuk komunikasi pada jaringan di internet dan berisi beberapa buah alamat *network* yang unik, sehingga tidak ada dua *Host* yang menggunakan alamat yang sama jika intranet tersebut telah terhubung ke internet. Ketika beberapa alamat publik telah ditetapkan, maka beberapa rute dapat diprogram ke dalam sebuah *router*, sehingga lalu lintas data yang menuju alamat publik tersebut dapat mencapai lokasinya. Di internet, lalu lintas sebuah alamat publik tujuan dapat dicapai, selama masih terkoneksi dengan jaringan internet.

b. IP *Private*

   IP *Private* adalah IP *address* yang digunakan untuk komunikasi yang tidak terhubung langsung dengan internet atau berada pada sebuah area lokal. Dengan menggunakan IP *private* ini, komputer

tidak dapat terhubung dengan internet dan hanya dapat bertukar infomasi dengan komputer lainnya yang juga terhubung pada jaringan yang sama. IP *private* ini digunakan pada jaringan LAN.

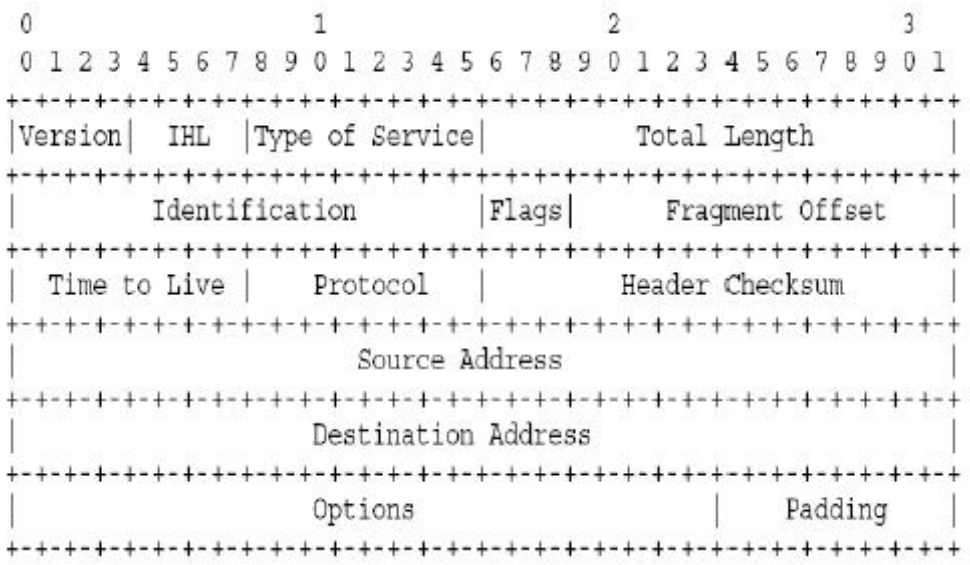
Berikut ini merupakan alamat IP *private* yang digunakan adalah sebagai Berikut ini merupakan :

Tabel 2.5 Alamat IP *Private* (cisco academy, 2010)

Kelas	Alamat IP
Kelas A	10.0.0.0 – 10.255.255.255
Kelas B	172.16.0.0 – 172.31.255.255
Kelas C	192.168.0.0 – 192.168.255.255

2.2.9.1 Struktur *Header Internet Protocol version 4*

Paket-paket data dalam protocol IP dikirimkan dalam bentuk datagram. Sebuah datagram IP terdiri atas *header* IP dan muatan IP. *Header* Ip menyediakan dukungan untuk memetakan jaringan (routing), mengidentifikasi muatan IP, ukuran *header* IP dan datagram IP, dukungan fragmentasi, dan juga IP Options. Sedangkan muatan IP memiliki ukuran berisi informasi yang dikirimkan. Muatan IP memiliki ukuran bervariasi, berkisar dari 8 *byte* hingga 65515 *byte*. Sebelum dikirimkan di dalam saluran jaringan, datagram IP akan dibungkus dengan *header* protokol lapisan antarmuka jaringan dan trailernya, untuk membuat sebuah frame jaringan. Menurut Lammle (2005), setiap datagram terdiri dari beberapa *field* yang memiliki fungsi tersendiri dan memiliki informasi yang berbeda-beda. Pada gambar berikut, dapat dilihat struktur *header* dari *header* IPv4.



Gambar 2.14 Format *Header IPv4*

Header IPv4 terdiri atas beberapa *field*, antara lain sebagai Berikut ini merupakan :

1. *Version* : digunakan untuk menindikasikan version dari *header* IP yang digunakan, yaitu IPv4.
2. *Internet Header Length* : digunakan untuk mengindikasikan ukuran *header* IP.
3. *Type of Service* : *field* ini digunakan untuk menentukan kualitas transmisi dari sebuah datagram IP.
4. *Total Length* : merupakan panjang total dari datagram IP, yang mencakup *header* IP dan muatannya.
5. *Identification* : digunakan untuk mengidentifikasi sebuah paket IP tertentu yang akan di fragmentasi.
6. *Flags* : berisi dua buah flag yang berisi apakah sebuah datagram IP mengalami fragmentasi atau tidak.

7. *Fragment Offset* : digunakan untuk mengidentifikasikan offset dimana fragmen yang bersangkutan dimulai, dihitung dari permulaan muatan IP yang belum pecah.
8. *Time to Live* : digunakan untuk mengidentifikasikan berapa banyak saluran jaringan dimana sebuah datagram IP dapat berjalan-jalan sebelum sebuah *router* mengabaikan datagram tersebut.
9. *Protocol* : digunakan untuk mengidentifikasikan jenis protokol lapisan yang lebih tinggi yang dikandung oleh muatan IP.
10. *Header Checksum* : filed ini berguna hanya untuk melakukan pengecekan integritas terhadap *header* IP.
11. *Source IP Address* : *field* ini mengandung alamat IP dari sumber *Host* yang mengirimkan datagram IP tersebut.
12. *Destination IP Address* : *field* ini mengandung alamat IP tujuan kemana datagram Ip tersebut akan disampaikan.
13. *Option* : fitur pendukung Ip yang dapat dipilih, biasanya fitur kemanan..
14. *Padding* : Bit-bit 0 tambahan yang ditambahkan ke dalam *field* ini untuk memastikan *header* IPv4 tetap berukuran 32 bit.

2.2.10 *Internet Protocol version 6 (IPv6)*

IPv6 atau IPng (*Internet Protocol Next Generation*) dirancang sebagai perbaikan dari *internet protocol* yang digunakan sekarang yaitu IPv4. IPv6 dapat diinstall seperti mengupgrade *software* biasa dan dapat dioperasikan bersama-sama dengan IPv4. IPv6 dirancang untuk bekerja dengan baik pada jaringan dengan perfomansi tinggi dan juga efisien untuk jaringan dengan *bandwidth* yang kecil seperti *wireless*. IPv6 juga menyediakan *platform* untuk fungsi-fungsi baru pada internet yang akan dibutuhkan di masa depan.[2][4]

Hal yang mendasari perlunya *internet protocol* versi baru adalah pertumbuhan internet yang semakin besar. IPv4 dapat dikatakan hanya digunakan pada pasar komputer. Pasar komputer telah menjadi pendorong pertumbuhan internet yang mencakup jaringan internet dan banyak lagi jaringan-jaringan internet kecil yang tidak terhubung ke internet. Pasar ini telah berkembang dengan tingkat pertumbuhan secara eksponensial. Pada 10 April 1994 jumlah jaringan yang terhubung ke internet adalah sebanyak 40.073 dan menjadi dua kalinya setiap tahun.

Pertumbuhan internet di masa yang akan datang, mungkin bukan didorong oleh pasar komputer sebagai pendorong utamanya. Salah satu pasar utama yang akan mendorong pertumbuhan internet adalah jaringan untuk hiburan *(entertainment)*, misalnya *chanel* untuk televisi, *video on demand*, dan sebagainya. Ada kemungkinan bahwa setiap pesawat televisi akan menjadi *Host internet*. Pasar yang besar ini akan membutuhkan protokol internet yang mendukung *routing* dan pengalamatan dalam skala besar, dan konfigurasi

otomatis. Pasar ini juga membutuhkan protokol-protokol yang memerlukan biaya minimum. Biaya akan menjadi faktor utama dalam pemilihan teknologi.

IPv6 dirancang sebagai perbaikan dari IPv4, dan bukan merupakan perubahan yang ekstrem dari IPv4. Fungsi-fungsi yang bekerja pada IPv4 juga ada pada IPv6, sedangkan fungsi-fungsi yang tidak bekerja pada IPv4 dihilangkan pada IPv6. Perubahan dari IPv4 ke IPv6 dapat dibagi dalam beberapa kategori, yaitu :

1. Kapabalitas *routing* dan pengalamatan yang semakin besar. Pengalamatan yang digunakan meningkat dari 32 bit pada IPv4 menjadi 128 bit pada IPv6 untuk mendukung hierarki pengalamatan dan jumlah pengalamatan node-node yang lebih banyak, dan konfigurasi alamat-alamat secara otomatis yang lebih sederhana.
2. Tipe alamat yang baru yang disebut *anycast address* didefinisikan untuk mengidentifikasi kumpulan node-node dimana paket yang dikirimkan ke sebuah *anycast address* dikirimkan ke salah satu node. Penggunaan *anycast address* pada rute sumber memungkinkan node-node mengontrol path tempat aliran traffic.
3. Penyederhanaan format *header*. Beberapa *field-field* pada *header* IPv4 telah dihilangkan atau lebih optional untuk mengurangi pemrosesan dari penanganan paket dan untuk menjaga *bandwidth* dari IPv6 sekecil mungkin walaupun ada peningkatan ukuran alamat. Walaupun panjang pengalamatan IPv6 empat kali panjang pengalamatan IPv4, panjang *header* IPv6 hanyalah dua kali panjang *header* IPv4.

4. Peningkatan dukungan untuk *option-option*. Perubahan pada penyedian *option-option* pada *header* IPv6 memungkinkan proses pelewatan paket yang lebih efisien, batasan-batasan panjang *option* yang lebih besar, dan fleksibilitas untuk *option-option* yang mungkin ada di masa depan.
5. Kapabilitas *Quality of Services* (QoS). Sebuah kapabilitas baru ditambahkan untuk memungkinkan pemberian label pada paket-paket dari aliran traffic tertentu dimana pengirim membutuhkan penanganan khusus, seperti *quality of service* yang bukan *default* dan *service* yang *bersifat real-time*.
6. Kapabilitas authentikasi dan privasi. IPv6 juga mendukung authentikasi, kesatuan data, dan kerahasiaan.

2.2.10.1 Struktur *Header Internet Protocol version 6*

IPv6 memiliki beberapa fitur yang mampu mengantisipasi perkembangan aplikasi masa depan dan mengatasi kekurangan yang dimiliki pendahulunya, yaitu IPv4. IPv6 dirancang sebagai perbaikan dari IPv4. *Header* pada Ipv6 terdiri dari dua jenis, yang pertama, yaitu *field* yang dibutuhkan oleh setiap paket disebut *header* dasar, sedangkan yang kedua yaitu *field* yang tidak selalu diperlukan pada packet disebut *header* ekstensi, dan *header* ini didifinisikan terpisah dari *header* dasar. *Header* dasar selalu ada pada setiap paket, sedangkan *header* tambahan hanya jika diperlukan diselipkan antara *header* dasar dengan data. *Header* tambahan, saat ini didefinisikan selain bagi penggunaan ketika paket dipecah, juga didefinisikan bagi fungsi sekuriti dan lain-lain. *Header* tambahan ini, diletakkan setelah *header* dasar, jika dibutuhkan beberapa *header* maka *header* ini akan

disambungkan berantai dimulai dari *header* dasar dan berakhir pada data. *Router* hanya perlu memproses *header* yang terkecil yang diperlukan saja, sehingga waktu pemrosesan menjadi lebih cepat. Hasil dari perbaikan ini, meskipun ukuran *header* dasar membesar dari 20 bytes menjadi 40 bytes namun jumlah *field* berkurang dari 12 menjadi 8 buah saja.

Berikut ini merupakan format *header* dari IPv6.



Gambar 2.15 Format *Header IPv6*

Field-field pada *header* IPv6 dapat dijelaskan secara singkat sebagai Berikut ini merupakan :

1. *Version* : *Field* 4 bit yang menunjukkan versi Internet Protokol, yaitu 6.
2. *Prior* : *Field* 4 bit yang menunjukkan nilai prioritas. *Field* ini memungkinkan pengirim paket mengidentifikasi prioritas yang diinginkan untuk paket yang dikirimkan, relatif terhadap paket-paket lain dari pengirim yang sama.

3. *Flow Label* : *Field* 24 bit yang digunakan oleh pengirim untuk memberi label pada paket-paket yang membutuhkan penanganan khusus dari *router* IPv6, seperti *quality of service* yang bukan default, misalnya *service-service* yang bersifat *real-time.*
4. *Payload Length* : *Field* berisi 16 bit yang menunjukkan panjang *payload*, yaitu sisa paket yang mengikuti *header* IPng, dalam oktet.
5. *Next Header* : *Field* 8 bit yang berfungsi mengidentifikasi *header* Berikut ini merupakan yang mengikuti *header* IPv6 utama.
6. *Hop Limit* : *Field* berisi 8 bit unsigned integer. Menunjukkan jumlah *link* maksimum yang akan dilewati paket sebelum dibuang. Paket akan dibuang bila *Hop Limit* berharga nol.
7. *Source Address* : *Field* 128 bit, menunjukkan alamat pengirim paket.
8. *Destination Address* : *Field* 128 bit, menunjukkan alamat penerima paket.

2.2.10.2 Arsitektur Pengalamatan IPv6

Alamat IPv6 adalah pengidentifikasi sepanjang 128 bit untuk *interface* dan sekumpulan *interface.* Ada tiga tipe pari pengalamatan IPv6.

1. *Unycast address :* Pengidentifikasi untuk *interface* tunggal. Paket yang dikirimkan ke alamat *unycast* adalah paket yang dikirim ke sebuah *interface* yang diidentifikasi oleh alamat tersebut.
2. *Anycast address :* Pengidentifikasi untuk sekumpulan *interface* (umumnya mili *node* yang berbeda). Paket yang dikirimkan ke alamat *anycast* adalah paket yang dikirimkan ke salah satu dari

sekumpulan *interface* yang diidentifikasi oleh alamat tersebut (alamat yang paling dekat, mengacu pada pengukuran jarak dari protokol *routing*).

3. *Multicast address :* Pengidentifikasi untuk sekumpulan *interface* (umumnya milik *node* yang berbeda). Paket yang dikirimkan ke alamat *multicast* adalah paket yang dikirimkan ke semua *interface* yang diidentifikasi oleh alamat tersebut.

2.2.10.3 Mekanisme Transisi IPv4 ke IPv6

Transisi dari IPv4 ke IPv6 harus selesai sebelum *routing* dan pengalamatan pada IPv4 melebihi batasannya. Tujuan utama dari transisi ini adalah bahwa IPv6 dan IPv4 dapat digunakan secara bersama-sama, *router* dan *Host* IPv6 dapat disebarkan secara bertahap dengan sedikit ketergantungan, dan transisi ini harus mudah dimengerti dan dilaksanakan oleh pengguna akhir, *system administrator* dan operator jaringan.[4][5]

Mekanisme transisi IPv6 menyediakan beberapa fitur, antara lain :

1. *Upgrade* dan penyebaran secara bertahap. *Host-Host* dan *router-router* IPv4 dapat diupgrade ke IPv6 secara bertahap tanpa keharusan mengupgrade *Host* atau *router* lain pada saat yang bersamaan.
2. Ketergantungan *upgrade* yang minimal. Satu-satunya persyaratan untuk mengupgrade *Host* ke IPv6 adalah *server* DNS harus lebih dulu diupgrade untuk menangani *record-record* alamat IPv6. Tidak ada keharusan untuk mengupgrade *router*.

3. Pengalamatan yang mudah. Pada waktu *Host* IPv4 diupgrade ke IPv6, *Host* tersebut tetap dapat menggunakan alamat lama. Tidak ada keharusan untuk menggunakan alamat baru.
4. Biaya mula yang murah.

Mekanisme transisi menjamin bahwa *Host* IPv6 dapat digunakan bersama *Host* IPv4 di jaringan internet. Fitur ini melindungi investasi untuk IPv4 dan tidak membuat IPv4 menjadi *absolute*. Transisi yang dapat dilakukan secara bertahap memungkinkan pengguna akhir dan operator jaringan untuk menyebarkan IPv6 sesuai jadwal masing-masing.

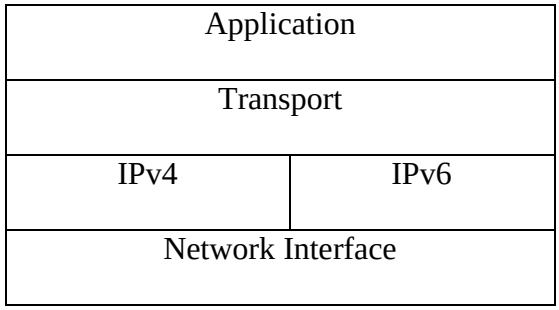
Sekarang ini, *Host-Host* yang menggunakan IPv6 dapat berkomunikasi di antara sesamanya dengan melalui jaringan internet yang masih menggunakan IPv4 melalui proses yang disebut *tunneling*. *Tunneling* ini adalah proses enkapsulasi IP di dalam IP, yaitu dengan menyisipkan *stack* IPv6 di atas *layer* IP pada IPv4 sehingga data dengan format data IPv6 dapat dikirimkan melalui jaringan yang masih menggunakan IPv4.

Ada beberapa alasan mengapa IPv6 tepat untuk *internet protocol* dimasa depan. IPv6 menyelesaikan masalah pengalamatan pada internet yang semakin berkembang, menyediakan mekanisme transisi yang fleksibel, dan dirancang untuk memenuhi kebutuhan pasar-pasar baru seperti jaringan hiburan dan peralatan pengendali. IPv6 melakukannya secara bertahap sehingga mengurangi resiko masalah arsitektur.

Ada beberapa mekanisme transisi yang dikenal antara lain *dual stack* dan *tunneling*.[3]

2.2.10.3.1 *Dual Stack IPv4/IPv6*

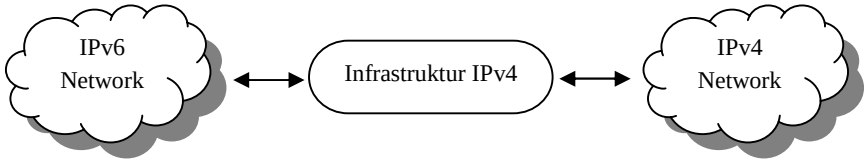
Dual stack adalah mekanisme yang mendukung kedua protokol IPv6 maupun IPv4 untuk *Host* dan *router*. Berikut ini merupakan adalah struktur umum *dual stack IPv4/IPv6.*



Gambar 2.16 *Dual Stack IPv4/IPv6*

2.2.10.3.2 *Tunneling*

Tunneling adalah sebuah mekanisme untuk menghubungkan dua jaringan yang berbeda. Secara umum *tunnelling* dapat dianalogikan dengan dua buah *Host.* 1 *Host* sumber dan 1 *Host* tujuan dan merupakan jaringan sama. Mekanisme *tunneling* yang digunakan yaitu dengan melewatkan paket IPv6 melalui jaringan IPv4 yang telah ada, tanpa merubah infrasuktur IPv4 yang telah ada.



Gambar 2.17 Mekanisme Transisi *Tunneling*

Ada beberapa mekanisme *tunneling* yang dikenal, antara lain *6over4, 6to4, tunnel broker,* dan *Dual Stack Transition Mechanism (DSTM).*

A. *6over4*

6over4 adalah pengiriman paket IPv6 dapat secara otomatis dienkapsulasi melalui jaringan IPv4 dengan menggunakan *IP Multicast.*

B. *6to4*

6to4 adalah alamat IPv6 dibuat berdasarkan alamat IPv4 atau disebut dengan *IPv4-compatible IPv6 compatible address.*

C. *Tunnel Broker*

Tunnel broker merupakan salah satu mekanisme transisi IPv4 ke IPv6 secara *tunneling* yaitu dengan menyediakan konfigurasi secara otomatis untuk melakukan *tunneling* IPv6 melalui IPv4 kepada *client* IPv4 yang terhubung ke jaringan internet. Jadi, *tunnel broker* dapat dianalogikan sebagai ISP dengan IPv6 sebagai penyedia koneksi IPv6 kepada *client* yang telah terhubung ke jaringan internet dengan menggunakan IPv4.

D. *Dual Stack Transition Mechanism (DSTM)*

Dual Stack Transition Mechanism yaitu alokasi IPv4 dilakukan secara otomatis, penggunaan IPv4 *over* IPv6 untuk pengiriman melalui IPv6 sebelum tersambung ke jaringan IPv4.

2.2.11 *IP Security (IPSec)*

IPSec didesain untuk menyediakan interoperabilitas, kualitas yang baik, *security* berbasis kriptografi untuk IPv4 dan IPv6. Layanan yang disediakan meliputi kontrol akses, integritas hubungan, autentifikasi data asal, proteksi jawaban lawan, kerahasiaan, dan pembatasan aliran lalu lintas kerahasiaan. Layanan-layanan ini tersedia dalam IP layer, memberi perlindungan pada IP dan *layer protocol* berikutnya. *IP Security* menyediakan sederet layanan untuk mengamankan komunikasi antar komputer dalam jaringan. Selain itu juga menambah integritas dan kerahasiaan, penerima jawaban optional dan autentifikasi data asal (melalui manajemen kunci SA), *IP Security* juga menyediakan kontrol akses untuk lalu lintas yang melaluinya[4][6].

Tujuan-tujuan ini dipertemukan melalui penggunaan dua protokol pengamanan lalu lintas yaitu AH (*Authentication Header*) dan ESP (*Encapsulating Security Payload*) dan dengan penggunaan prosedur dan protokol manajemen kunci kriptografi. Jika mekanisme ini diimplementasikan sebaiknya tidak merugikan pengguna, *host* dan komponen internet lainnya yang tidak menggunakan mekanisme ini untuk melindungi lalu lintas data mereka. Mekanisme ini harus fleksibel dalam menggunakan algoritma keamanan, maksudnya yaitu modul ini dapat menggunakan algoritma sesuai dengan pilihan tanpa mempengaruhi komponen implementasi lainnya. Penggunaan algoritma defaultnya harus dapat memfasilitasi interoperabilitas dalam internet pada umumnya. Penggunaan algoritma ini dalam hubungannya dengan proteksi lalu lintas (*IPSec traffic protection*) dan protokol manajemen kunci (*key management*

protocols), bertujuan memperbolehkan sistem dan pengembang aplikasi untuk meningkatkan kualitas yang tinggi, *internet layer*, teknologi keamanan berbasis kriptografi.

IPSec protokol yang dikombinasikan dengan algoritma *default*-nya didesain untuk menyediakan keamanan lalu lintas internet yang baik. Bagaimanapun juga keamanan yang diberikan oleh protokol ini sebenarnya bergantung pada kualitas dari implementasi, yang mana implementasi ini diluar lingkup dari standarisasi ini. Selain itu keamanan sistem komputer atau jaringan adalah fungsi dari banyak faktor meliputi individu, fisik, prosedur, dan praktek keamanan komputer dalam dunia nyata. IPSec hanya salah satu komponen dari arsitektur sistem keamanan. Keamanan yang didapat dari pemakaian IPSec bergantung pada lingkungan operasi dimana implementasi IPSec dijalankan.

2.2.11.1 Definisi IPSec

IPSec menyediakan layanan sekuritas pada IP layer dengan mengizinkan sistem untuk memilih protokol keamanan yang diperlukan, memperkirakan algoritma apa yang akan digunakan pada layanan, dan menempatkan kunci kriptografi yang diperlukan untuk menyediakan layanan yang diminta. IPSec dapat digunakan untuk memproteksi satu atau lebih path antara sepasang *Host*, antara sepasang *security gateway*, atau antara *security gateway* dengan *Host*.

Layanan dari sekuritas yang disediakan oleh IPSec meliputi kontrol akses, integritas dan lain-lain seperti pada bagian atas bekerja pada IP layer oleh karena itu layanan ini dapat digunakan oleh *layer protocol* yang lebih tinggi seperti TCP,

UDP, ICMP, BGP dan lain-lain. IPSec DOI juga mendukung kompresi IP [SMPT 98] dimotivasi dari pengamatan bahwa ketika kompresi diterapkan dalam IPSec, hal ini akan mencegah kompresi efektif pada protokol yang lebih rendah.

2.2.11.2 Mekanisme IPSec

IPSec menggunakan dua protokol untuk menyediakan layanan keamanan lalu lintas yaitu *Authentication Header* (AH) dan *Encapsulating Security Payload* (ESP). Implementasi IPSec harus mendukung ESP dan juga AH.

a. Protokol AH menyediakan integritas hubungan, autentifikasi data asal dan layanan anti jawaban.
b. Protokol ESP menyediakan kerahasiaan, dan pembatasan aliran lalu lintas kerahasiaan. ESP juga menyediakan layanan integritas hubungan, autentifikasi data asal dan layanan anti jawaban.
c. Kedua protokol ini merupakan pembawa kontrol akses berbasis distribusi kunci kriptografi dan manajemen aliran lalu lintas relatif terhadap protokol keamanan.

Protokol-protokol ini dapat diterapkan secara sendiri-sendiri atau dikombinasikan antara keduanya untuk menyediakan layanan keamanan yang diinginkan dalam IPv4 dan IPv6. Masing-masing protokol mendukung dua mode penggunaan: *mode transport* dan *mode tunnel*. Dalam *mode transport* protokol menyediakan proteksi terutama untuk *layer protocol* berikutnya. Sedangkan dalam *mode tunnel* protokol diterapkan untuk meneruskan paket IP. Perbedaan antara kedua mode tersebut dijelaskan pada bagian berikutnya.

IPSec mengizinkan administrator sistem untuk mengontrol bagian-bagian terkecil dimana layanan keamanan diberikan. Sebagai contoh, salah satu dapat membuat tunnel enkripsi tunggal untuk membawa semua lalu lintas antara dua *security gateway* atau membuat tunnel enkripsi terpisah yang dibuat di masing-masing hubungan TCP antara sepasang *host* yang berkomunikasi melintasi *gateway* tersebut. Manajemen IPSec harus menggabungkan fasilitas untuk menspesifikasikan:

a. Layanan keamanan yang digunakan dan dengan kombinasi yang seperti apa.
b. Bagian sekecil apa proteksi keamanan diterapkan.
c. Algoritma yang digunakan untuk mempengaruhi keamanan berbasis kriptografi.

Karena layanan keaman ini menggunakan nilai rahasia yang di-*shar*e (*cryptographic keys*), IPSec mengandalkan mekanisme terpisah untuk menempatkan kunci ini.

2.2.11.3 Implementasi IPSec

Ada berbagai macam cara pengimplementasian IPSec dalam *host* atau hubungan dengan firewall atau *router*.

Beberapa contoh implementasi tersebut dijelaskan dibawah ini:

a. Integrasi IPSec kedalam implementasi native IP. Cara ini membutuhkan akses ke source code IP dan cara ini mudah diaplikasikan untuk *host* dan *security gateway*.

b. Implementasi *Bump-In-The-Stack (BITS)*, dimana IPSec diimplementasikan dibawah implementasi protokol stack IP yang sudah ada, diantara native IP (IP asli) dan driver jaringan lokal. Akses *source code* untuk IP stack tidak diperlukan dalam konteks ini, membuat implementasi ini mendekati penggunaan yang sesuai dengan sistem pewarisan. Pendekatan ini kita digunakan, pada umumnya digunakan dalam *host*.

c. Penggunaan pengolah *kriptografi outboard* merupakan desain keamanan jaringan yang umum digunakan oleh militer dan beberapa sistem komersil. Sistem ini kadang dikenal sebagai implementasi *Bump-In-The-Wire (BITW).* Implementasi seperti itu dirancang untuk melayani *host* atau *gateway*. Biasanya *device BITW* adalah IP petunjuk. Apabila menyokong hanya *host* tunggal maka analogi dengan BITS, tapi apabila menyokong *router* atau *firewall* maka harus berperilaku sebagai *security gateway*.

2.2.11.4 *Security Association*

Kebutuhan manajemen untuk implementasi IPv6 dan implementasi IPv4 yang mengimplementasikan AH, ESP atau keduanya. Konsep "*Security Association*" adalah pokok dari IPSec. Semua implementasi dari AH dan ESP harus mendukung konsep *Security.* Bagian terakhir menguraikan berbagai aspek manajemen *security association,* mendefinisikan manajemen kebijakan SA yang diperlukan, proses lalu lintas, dan teknik manajemen SA.

Security Association adalah suatu hubungan simplex yang menghasilkan layanan keamanan lalu lintas yang dibawanya. Layanan keamanan ini dihasilkan oleh SA dengan penggunaan AH atau ESP tapi bukan penggunaan keduanya. Jika proteksi AH dan ESP diterapkan dalam aliran lalu lintas, kemudian dua tau lebih SA di-*create* untuk menghasilkan proteksi dalam aliran lalu lintas. Untuk mengamankan komunikasi dua arah antara dua *Host*, atau antara dua *security gateway* maka dibutuhkan dua SA.

Security Association secara unik dikenali dari tiga komponen yaitu Security Parameter Index (SPI), alamat tujuan IP dan protokol keamanan (AH atau ESH). Nilai SPI mencakup nilai 1 sampai 255 yang ditetapkan oleh IANA (Internet Assigned Number Authority) untuk penggunaan dimasa yang akan datang. Nilai SPI nol (0) ditetapkan untuk penggunaan implementrasi khusus lokal dan tidak dikirim lewat kabel. Sebagai contoh implementasi manajemen kunci mempunyai nilai SPI nol yang berarti tidak ada *security association* selama periode ketika implementasi IPSec telah meminta bahwa entitas manajemen kunci tersebut menetapakan SA baru, tetapi SA belum masih belum ditetapkan.

Pada prinsipnya, alamat tujuan merupakan *unycast address*, *IP broadcast address* atau *multicat group address*. Bagaimanapun mekanisme manajemen SA IPSec saat ini hanya didefinisikan untuk SA *unycast*. Oleh karena itu, untuk diskusi pemaparan selanjutnya SA dideskripsikan utamanya untuk komunikasi *point-to-point*, meskipun konsepnya dapat diaplikasikan untuk kasus komunikasi *point-to-multipoint*. Didefinisikan dua tipe SA yaitu *mode transport* dan *mode tunnel*. SA *mode transport* adalah SA antara dua *host*.

Dalam kasus dimana *link security* ingin digunakan antara dua sistem intermediate sepanjang path *mode transport* juga dapat digunakan antara dua *security gateway*. Dalam kasus terbaru *mode transport* juga digunakan untuk mensuport IP-in-IP atau GRE tunneling melalui SA *mode transport*.

Catatan bahwa fungsi kontrol akses merupakan bagian yang penting dari IPSec secara significan dibatasi dalam konteks ini. Sehingga penggunaan *mode transport* harus dievaluasi secara hati-hati sebelum digunakan. Dalam IPv4, *header* protokol keamanan *mode transport* terlihat setelah *header* IP dan beberapa pilihan lain dan sebelum protokol layer yang lebih tinggi (seperti TCP atau UDP) dalam IPv6, *header* protokol keamanan terlihat setelah *header* base IP dan ekstensionnya, tetapi mungkin juga terlihat sebelum atau sesudah pilihan tujuan dan sebelum protokol layer yang lebih tinggi.

Dalam kasus ESP SA *mode tranport* menyediakan layanan keamanan hanya untuk protokol layer yang lebih tinggi darinya, tidak untuk IP *header* atau ekstension *header* yang mendahului ESP *header*. Dalam kasus untuk AH, proteksi juga ditambahkan ke bagian yang dipilih dari IP *header*, bagian yang dipilih dari ekstension *header* dan option pilihan (yang terdapat pada *header* IPv4, Hop-by-Hop ekstension *header* IPv6, atau ekstension *header* tujuan pada IPv6).

SA *mode tunnel* adalah SA yang diaplikasikan di IP tunnel. Dengan hanya sepasang pengecualian, kapan saja ujung manapun dari SA adalah *Security gateway*, SA harus *mode tunnel*. SA diantara dua *security gateway* pada dasarnya adalah SA *mode tunnel* seperti SA antara *host* dan *security gateway*. Catatan bahwa dalam kasus dimana lalu lintas ditujukan untuk *security gateway* seperti

SNMP *commands*, *security gateway* berlaku sebagai *host* dan *mode transport* diperbolehkan.

Tapi dalam kasus tersebut *security gateway* tidak berlaku sebagai *gateway*. *Security gateway* mungkin mendukung *mode transport* untu menyediakan *link* keamanan. Dua *host* dapat menyusun sebuah *mode tunnel*. Kebutuhan untuk *transit traffic* SA meliputi *security gateway* untuk menjadi SA tunnel mengacu ke kebutuhan untuk menghindari problem potensial dengan memperhatikan fragmentasi dan penyusunan ulang dari paket IPSec dan dalam keadaan dimana *path* yang banyak menuju ke tujuan yang sama di belakang *security gateway*. Untuk SA *mode tunnel* ada *header* IP luar yang menspesifikasikan pemrosesan tujuan IPSec ditambah dengan *header* IP dalam yang menunjukkan tujuan terakhir dari peket tersebut. *Header* protokol keamanan terlihat setelah *header* IP luar dan sebelum *header* IP dalam.

Jika AH diterapkan dalam *mode tunnel* bagian *header* IP luar diperoleh proteksi seperti halnya paket IP yang disalurkan. Jika ESP diterapkan proteksi, maka dikerjakan hanya pada paket yang disalurkan tidak pada *header* luar.

2.2.11 .5 *Fungsi Security Association*

Layanan keamanan yang diberikan oleh SA bergantung pada protokol *security* yang dipilih, *mode SA*, *endpoint* SA, dan pada pemilihan layanan optional yang disertakan dalam protokol. Sebagai contoh, AH menyediakan layanan autentifikasi data asal dan integritas hubungan untuk datagram IP. AH juga memberikan layanan anti-replay, untuk membantu *counter* menolak *service*

attack. AH merupakan protokol yang cocok untuk diterapkan jika kerahasiaan kurang dipedulikan. AH juga menyediakan autentifikasi untuk bagian yang dipilih dari *header* IP. Sebagai contoh, jika integritas dari sebuah *header option* IPv4 atau *header ekstension* IPv6 harus diproteksi dalam rute antara pengirim dan penerima, AH menyediakan layanan tersebut.

ESP menyediakan kerahasiaan untuk lalu lintas. ESP juga menyediakan layanan autentifikasi. Jika autentifikasi dirundingkan untuk SA ESP, penerima juga memilih untuk menguatkan layanan anti-reply dengan fitur yang sama seperti layanan anti-reply pada AH. Jangkauan autentifikasi yang diberikan oleh ESP lebih dangkal daripada AH, seperti *header* IP yang berada diluar *header* ESP tidak terlindungi. Hanya jika protokol *layer* berikutnya perlu untuk diautentifikasi, maka autentifikasi ESP merupakan pilihan yang tepat dan akan lebih efisien ruang daripada AH. Perlu diingat meskipun kerahasiaan dan autentifikasi merupakan layanan optional tetapi kedua layanan tersebut tidak dapat dihilangkan.

Apabila layanan kerahasiaan (*confidentiality*) dipilih, maka SA ESP (*mode tunnel*) antara dua *security gateway* dapat memberikan kerahasiaan aliran lalu lintas parsial. Penggunaan *mode tunnel* menperbolehkan *header* IP dalam (inner IP *header*) untuk dienkripsikan, merahasiakan identitas dari sumber dan tujuan dari lalu lintas tersebut. Lebih dari, lapisan ESP *payload* juga dapat dilibatkan untuk menyembunyikan ukuran dari peket. Layanan *confidentiality* aliran lalu lintas yang sama juga dapat diberikan ketika *mobile user* menggunakan alamat *IP dynamic* dalam konteks dialup, dan menetapkan SA ESP (*mode tunnel*) menjadi *firewall.*