BAB 2
TINJAUAN PUSTAKA

2.1 Profil Instansi

BPPTKPK Jawa Barat (Balai Pelatihan Pendidik dan Tenaga Kependidikan Pendidikan Kejuruan) adalah unit pelaksana teknis di bawah Dinas Pendidikan Jawa Barat, yang bertanggung jawab kepada kepala Dinas Pendidikan Jawa Barat. BPPTKPK memiliki tugas pokok dan fungsi pada, Bab IV, Pasal 11 ayat (1) dan ayat (2)

1. Memimpin, mengkordinasikan dan mengendalikan pelaksanaan kegiatan pengembangan teknologi pendidikan.
2. Pengaturan teknis operasional di balai pengembangan teknolgi pendidikan.
3. Mengendalikan tugas-tugas dibidang pengembangan teknologi pendidikan yang meliputi perencanaan, pelatihan, penilaian dan uji coba model dan sistem pemebelajaran serta media pembelajaran.

2.1.1 Visi dan Misi

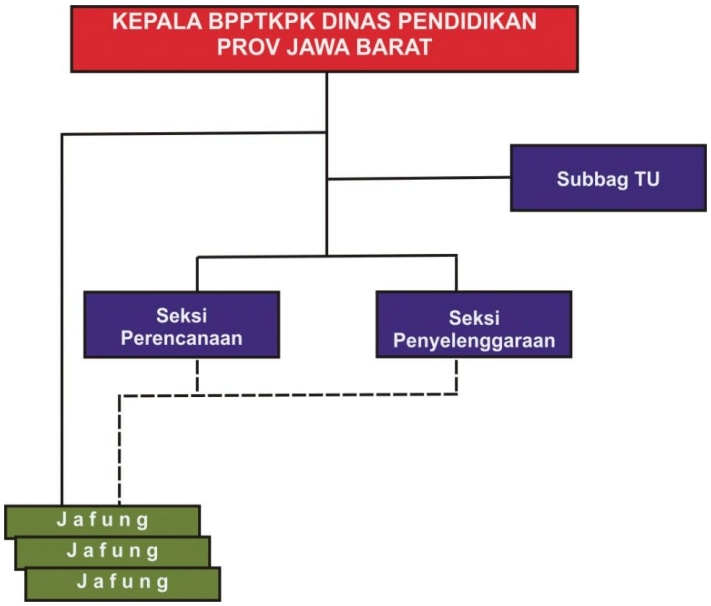
a. Visi

   "Akselerasi Peningkatan Mutu Pendidikan Kejuruan menuju masyarakat Jawa Barat yang Bertaqwa, Mandiri, Dinamis dan Sejahtera"

b. Misi

   1. Optimalisasi dan pengembangan sumberdaya kelembagaan dalam upaya meningkatkan layanan pendidikan kejuruan secara produktif, efektif, efisien dan akuntabel.
   2. Meningkatkan mutu, daya saing dan relevansi pendidikan melalui layanan pelatihan pendidik dan tenaga kependidikan Pendidikan kejuruan yang menguasai teknologi dan berwawasan global.

2.1.2 Struktur Organisasi



Gambar 2.1.2.1 Struktur Organisasi BPPTKPK

2.1.3 Deskripsi Kerja

1. Kepala BPPTKPK
   a. Tugas Pokok

      Memimpin, mengkoordinasikan, dan memotivasi serta mengawasi ruang lingkup tugas pokok Balai Pelatihan Pendidik dan Tenaga Kependidikan Pendidikan Kejuruan (BPPTKPK) Dinas Provinsi Jawa Barat dan memberikan keleluasan kepada 26 kabupaten Jawa Barat untuk melakukan pelatihan

   b. Fungsi

      Kepanjangan tugas dan Dinas Pendidikan Provinsi Jawa Barat untuk pengembangan teknologi umum dan teknologi pendidikan

2. Sub Bagian Tata Usaha

   Sub Bagian Tata usaha mempunyai tugas membantu Kepala BPPTKPK di bidang ketatausahaan, kepegawaian, keuangan, perlengkapan umum serta perencanaan dan pelaporan dalam administrasi manajemen Balai dan mengawasi struktural dalam pelaksanaan tugas pokok BPPTKPK.

3. Seksi Perencanaan

   Tugas pokoknya adalah merencanakan pengembangan program model dan sistem pembelajaran, mengevaluasi, memantau dan membina pemanfaatan teknologi informasi untuk pendidikan serta program perencanaan dalam jangka pendek dan jangka panjang.

4. Seksi penyelenggara

   Tugas pokok dari seksi penyelenggara yaitu mengumpulkan, menghimpun, menganalisa, serta menyusun rencana, dan melaksanakan program pelatihan guru atau siswa.

5. Kelompok Jabatan Fungsional

   Kelompok Jabatan Fungsional mempunyai tugas pokok melaksanakan proses pembelajaran kepada seluruh SMK terdiri dari sejumlah jabatan fungsional yang terbagi dalam berbagai kelompok sesuai dengan bidang keahliannya. Kelompok Jabatan fungsional di BPPTKPK ada 6 Jabatan Fungsional dalam data ketenagaan sesuai dengan keahliaannya sebagai berikut:

   a. Installasi Bangunan
   b. Installasi Listrik
   c. Installasi Mesin
   d. Installasi Elektronika
   e. Installasi Multimedia
   f. Installasi Otomotif

2.2 Konsep Jaringan Komputer

Jaringan komputer adalah himpunan “interkoneksi” antara dua komputer atau lebih yang terhubung dengan media transmisi kabel. Dua unit komputer atau lebih dikatakan terkoneksi apabila keduanya bisa saling bertukar data atau informasi, berbagi *resource* yang dimiliki seperti *file, printer,* dan media penyimpanan [2].

2.3 Jenis-Jenis Jaringan Komputer

Adapun jenis-jenis dari jaringan komputer dapat dibagi menjadi tiga bagian yaitu [2] :

1. *Local Area Network* (LAN)

   Sebuah LAN, adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan, seperti kantor pada sebuah gedung, atau tiap-tiap ruangan pada sebuah sekolah. Biasanya jarak antar node tidak lebih jauh dari sekitar 200 m.

2. *Metropolitan Area Network* (MAN)

   Sebuah MAN, biasanya meliputi area yang lebih besar dari LAN, misalnya antar gedung dalam suatu daerah (wilayah seperti propinsi atau negara bagian). Dalam hal ini jaringan menghubungkan beberapa buah jaringan kecil ke dalam lingkungan area yang lebih besar, sebagai contoh yaitu: jaringan beberapa kantor cabang sebuah bank didalam sebuah kota besar yang dihubungkan antara satu dengan lainnya.

3. *Wide Area Network* (WAN)

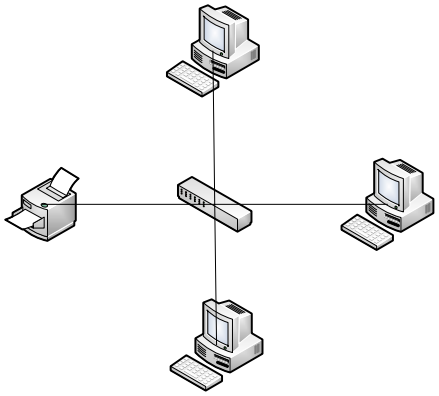
   Wide Area Network (WAN) adalah jaringan yang biasanya sudah menggunakan media wireless, sarana satelit ataupun kabel serat optic, karena jangkauannya yang lebih luas, bukan hanya meliputi satu kota atau antar kota dalam suatu wilayah, tetapi mulai menjangkau area/wilayah otoritas negara lain.

2.4 Arsitektur Jaringan Komputer

Arsitektur jaringan komputer adalah tata cara bagaimana penggunaan perangkat keras dan perangkat lunak dalam jaringan agar satu komputer dengan komputer lainnya dapat melakukan komunikasi dan pertukaran data. Berikut ini tiga arsitektur jaringan komputer yang paling umum digunakan [2].

1. Jaringan *Peer To Peer*

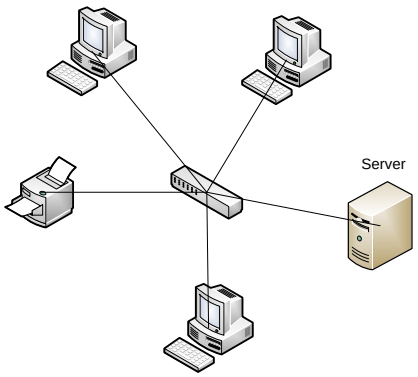
   Pada jaringan *peer to peer*, semua komputer memiliki posisi setara/sejajar, dalam hierarki yang sama. Setiap komputer dapat menjadi klien terhadap komputer *peer* lainnya, setiap komputer dapat pula berbagi sumber daya dengan komputer yang berada dalam jaringan *peer to peer* ini. Sumber daya diletakkan secara desentralisasi pada setiap anggota jaringan, dan tidak memerlukan administrator jaringan. Arsitektur jaringan *peer to peer* biasanya digunakan untuk jaringan yang kecil.



Gambar 2.4.1 Peer To Peer

1. Jaringan *Client / Server*

Pada jaringan client/server, perangkat lunak yang mengontrol keseluruhan kerja jaringan berada pada server. Jaringan ini dapat menghubungkan ratusan komputer dengan tingkat keamanan yang tidak memungkinkan berada pada arsitektur *peer to peer*. Untuk mendapatkan akses pada jaringan, *client* harus *login* atau melakukan autentikasi agar bisa mengakses sumber daya.

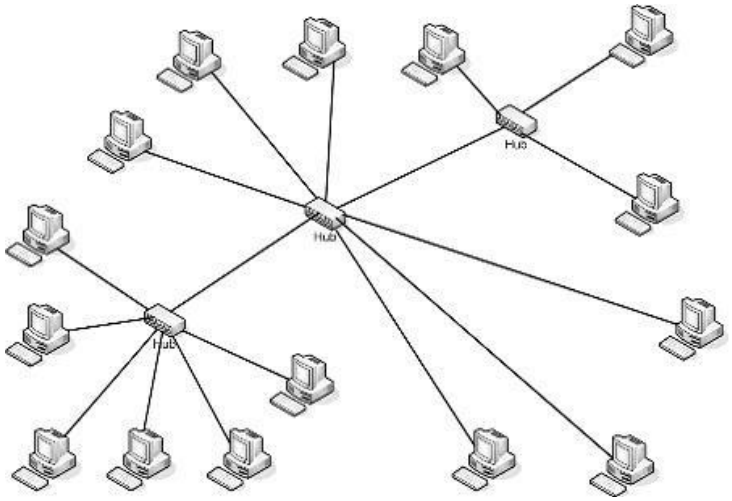


Gambar 2.4.2 Client Server

2. Jaringan *Hybrid*

Jaringan ini merupakan gabungan dari *peer to peer* dan *client/server*. Pada jaringan ini, Workgroup yang terdiri dari beberapa komputer yang saling terhubung dapat mengelola sumber daya tanpa membutuhkan

otorisasi dari administrator jaringan atau server. Pada jaringan ini, terdapat pula sifat dari jaringan *client/server* sehingga tingkat keamanan dapat lebih terjaga.



Gambar 2.4.3 Hybrid

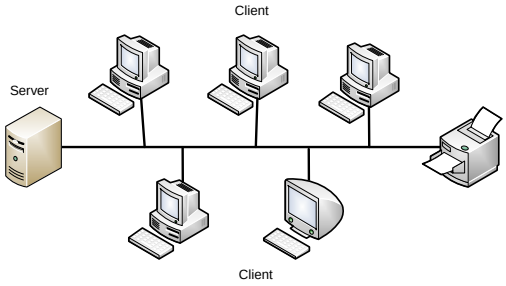
2.5 Topologi Jaringan

Topologi jaringan dapat dikatakan juga sebagai arsitektur jaringan. Topologi jaringan adalah gambaran perencanaan hubungan antar komputer dalam cakupan *Local Area Network*, yang umumnya menggunakan media transmisi kabel dan konektor seperti, ethernet card dan perangkat pendukung lainnya. Terdapat beberapa topologi jaringan yang sering digunakan yaitu :

2.5.1 Topologi BUS

Topologi ini merupakan bentangan satu kabel yang kedua ujungnya ditutup, dimana sepanjang kabel terdapat node-node. Signal dalam kabel dengan topologi ini dilewati satu arah sehingga memungkinkan sebuah collision terjadi [2].

1. Keuntungan Topologi BUS
    a. Murah, karena tidak banyak menggunakan media dan kabel yang digunakan banyak dipasaran.
    b. Setiap komputer dapat berhubungan secara langsung.
2. Kerugian Topologi BUS
    a. Sering terjadi hang / crass talk, yaitu bila lebih dari satu pasang memakai jalur diwaktu yang sama, harus bergantian atau ditambah relay.



Gambar 2.5.1.1 Topologi BUS [2]

2.5.2 Topologi Ring

Semua komputer saling tersambung membentuk lingkaran (seperti bus tetapi ujung-ujung bus disambung). Data yang dikirim diberi address tujuan sehingga dapat menuju komputer yang dituju. Tiap stasiun (komputer) dapat diberi repeater (transceiver) yang berfungsi sebagai [2]:

1) Listen State

   Tiap bit dikirim kembali dengan mengalami delay waktu.

2) Transmit State

   Bila bit yang berasal dari paket lebih besar dari ring maka repeater akan mengembalikan ke pengirim. Bila terdapat beberapa paket dalam ring, repeater yang tengah memancarkan, menerima bit dari paket yang tidak dikirimnya harus menampung dan memancarkan kembali.

3) Bypass State

   Berfungsi untuk menghilangkan delay waktu dari stasiun yang tidak aktif.

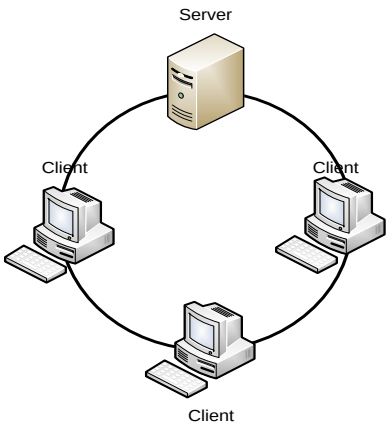
   1. Keuntungan Topologi Ring

      a. Kegagalan koneksi akibat gangguan media, dapat diatasi dengan jalur lain yang masih terhubung.

      b. Penggunaan sambungan point to point membuat transmission error dapat diperkecil

   2. Kerugian Topologi Ring

      a. Data yang dikirim bila melalui banyak komputer, transfer data menjadi lambat.



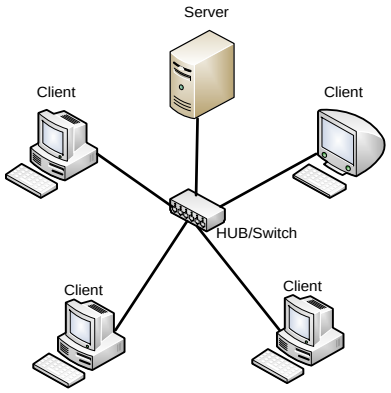
Gambar 2.5.2.1 Topologi Ring [2]

2.5.3 Topologi Star

Karakteristik dari topologi jaringan ini adalah node (station) berkomunikasi langsung dengan station lain melalui central node (hub/switch), traffic data mengalir dari node ke central node dan diteruskan ke node (station) tujuan. Jika salah satu segmen kabel putus, jaringan lain tidak akan terputus [2].

1. Keuntungan Topologi Star
    a. Akses ke station lain (client atau server) cepat
    b. Dapat menerima workstation baru selama port di centralnode (hub/switch) tersedia.
    c. Hub/Switch bertindak sebagai konsentrator.
    d. Hub/switch dapat disusun seri (bertingkat) untuk menambah jumlah station yang terkoneksi di jaringan.
    e. User dapat lebih banyak dibanding topologi bus, maupun ring
2. Kerugian Topologi Star
    a. Apabila traffic data cukup tinggi dan terjadi collision, maka semua komunikasi akan ditunda, dan koneksi akan dilanjutkan atau dipersilahkan dengan cara random, apabila hub/switch mendetect tidak ada jalur yang sedang dipergunakan oleh node lain.

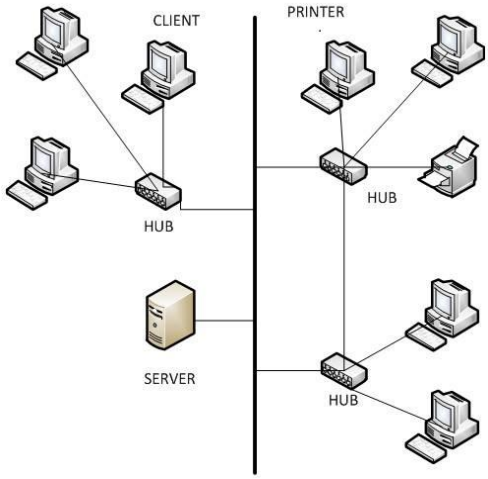
b. Apabila Hub/Switch rusak, koneksi jaringan akan berhenti.



Gambar 2.5.3.1 Topologi Star [2]

2.5.4 Topologi Tree

Tidak semua stasiun mempunyai kedudukan yang sama. Stasiun yang kedudukannya lebih tinggi menguasai stasiun dibawahnya, sehingga jaringan sangat tergantung dengan stasiun yang kedudukannya lebih tinggi (hierachical topology) dan kedudukan stasiun yang sama disebut *peer topology* [2].



Gambar 2.5.4.1 Topologi Tree [2]

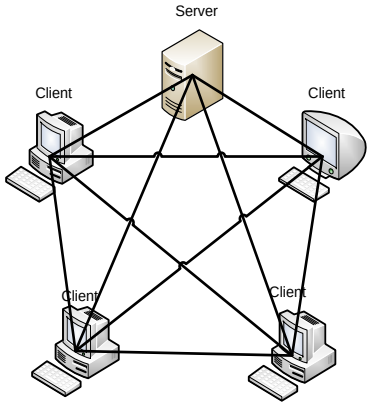
2.5.5 Topologi Mesh

Topologi jaringan ini menerapkan hubungan antar sentral secara penuh. Jumlah saluran harus disediakan untuk membentuk jaringan Mesh adalah jumlah

sentral dikurangi 1 (n-1, n = jumlah sentral). Tingkat kerumitan jaringan sebanding dengan meningkatnya jumlah sentral yang terpasang. Dengan demikian disamping kurang ekonomis juga relatif mahal dalam pengoperasiannya [2].

Topologi mesh ini merupakan teknologi khusus (ad hock) yang tidak dapat dibuat dengan pengkabelan, karena sistemnya yang rumit, namun dengan teknologi wireless topologi ini sangat memungkinkan untuk diwujudkan (karena dapat dipastikan tidak akan ada kabel yang berserakan).

Biasanya untuk memperkuat sinyal transmisi data yang dikirimkan, ditengah-tengah (area) antar komputer yang kosong di tempatkan perangkat radio (air point) yang berfungsi seperti repeater untuk memperkuat sinyal sekaligus bisa mengatur arah komunikasi data yang terjadi.



Gambar 2.5.5.1 Topologi Mesh [2]

2.6 Protokol Jaringan

Protokol merupakan himpunan aturan-aturan yang memungkinkan komputer satu dapat berhubungan dengan komputer lain. Aturan-aturan ini meliputi tatacara bagaimana agar komputer bisa saling berkomunikasi [2]. Berikut ini beberapa protokol yang banyak digunakan pada jaringan :

2.6.1 TCP/IP Protocols

Protokol TCP/IP merupakan dasar teknis dari internet. Pengembangan TCP/IP dimulai sebagai proyek DOD. Sekarang, sebagian besar protokol yang dikembangkan oleh *Internet Engineering Task Force* (IETF) di bawah *Internet Architecture Board* (IAB), adalah sebuah organisasi yang awalnya disponsori oleh

pemerintah AS, dan sekarang organisasi tersebut adalah organisasi yang terbuka dan otonom. Arsitektur TCP/IP tidak sama persis dengan model OSI layer. Sayangnya, tidak ada kesepakatan universal tentang bagaimana untuk menggambarkan TCP/IP dengan model OSI layer [3]. Berikut ini lapisan TCP/IP yang dipetakan dengan model OSI layer atau disebut juga dengan TCP/IP *Protocol Stack* [3]:

A. *Application Layer*
    1. BOOTP: *Bootstrap Protocol*
    2. DCAP*: Data Link Switching Client Access Protocol*
    3. DHCP: *Dynamic Host Configuration Protocol*
    4. DNS: *Domain Name Systems*
    5. FTP: *File Transfer Protocol*
    6. Finger: *User Information Protocol*
    7. HTTP: *Hypertext Transfer Protocol*
    8. S-HTTP: *Secure Hypertext Transfer Protocol* (S-HTTP)
    9. IMAP & IMAP4: *Internet Message Access Protocol*
    10. IPDC: IP *Device Control*
    11. IRCP (IRC): *Internet Relay Chat Protocol*
    12. LDAP: *Lightweighted Directory Access Protocol*
    13. MIME (S-MIME): *Multipurpose Internet Mail Extensions* (*Secure* MIME)
    14. NAT: *Network Address Translation*
    15. NNTP: *Network News Transfer Protocol*
    16. NTP: *Network Time Protocol*
    17. POP & POP3: *Post Office Protocol* (*version* 3)
    18. RLOGIN: *Remote Login in Unix*
    19. RMON: *Remote Monitoring* MIBs *in* SNMP
    20. SLP: *Service Location Protocol*
    21. SMTP: *Simple Mail Transfer Protocol*
    22. SNMP: *Simple Network Management Protocol*
    23. SNTP: *Simple Network Time Protocol*
    24. TELNET: TCP/IP *Terminal Emulation Protocol*

25. TFTP: *Trivial File Transfer Protocol*
26. URL: *Uniform Resource Locator*
27. X-*Window*: X *Window or* X *Protocol or* X *System*

B. *Presentation Layer*

1. LPP: *Lightweight Presentation Protocol*

C. *Session Layer*

1. RPC: *Remote Procedure Call protocol*

D. *Transport Layer*

1. ITOT: ISO *Transport Over* TCP/IP
2. RDP: *Reliable Data Protocol*
3. RUDP: *Reliable* UDP
4. TALI: *Transport Adapter Layer Interface*
5. TCP: *Transmission Control Protocol*
6. UDP: *User Datagram Protocol*

E. *Network Layer*

a) *Routing*

1. BGP/BGP4: *Border Gateway Protocol*
2. EGP: *Exterior Gateway Protocol*
3. IP: *Internet Protocol*
4. IPv6: *Internet Protocol version* 6
5. ICMP/ICMPv6: *Internet Control Message Protocol*
6. IRDP: *ICMP Router Discovery Protocol*
7. Mobile IP: IP *Mobility Support Protocol for* IPv4 & IPv6
8. NARP: *NBMA Address Resolution Protocol*
9. NHRP: *Next Hop Resolution Protocol*
10. OSPF: *Open Shortest Path First*
11. RIP (RIP2): *Routing Information Protocol*
12. RIPng: RIP *for* IPv6
13. RSVP: *Resource ReSerVation Protocol*
14. VRRP: *Virtual Router Redundancy Protocol*

b) *Multicast*

1. BGMP: *Border Gateway Multicast Protocol*
2. DVMRP: *Distance Vector Multicast Routing Protocol*
3. IGMP: *Internet Group Management Protocol*
4. MARS: *Multicast Address Resolution Server*
5. MBGP: *Multiprotocol* BGP
6. MOSPF: *Multicast* OSPF
7. MSDP: *Multicast Source Discovery Protocol*
8. MZAP: *Multicast-Scope Zone Announcement Protocol*
9. PGM: *Pragmatic General Multicast Protocol*
10. PIM-DM: *Protocol Independent Multicast - Dense Mode*
11. PIM-SM: *Protocol Independent Multicast - Sparse Mode*

c) MPLS *Protocols*

1. MPLS: *Multi-Protocol Label Switching*
2. CR-LDP: *Constraint-Based Label Distribution Protocol*
3. LDP: *Label Distribution Protocol*
4. RSVP-TE: *Resource ReSerVation Protocol-Traffic Engineering*

F. *Data Link Layer*

1. ARP *and* InARP: *Address Resolution Protocol and Inverse* ARP
2. IPCP *and* IPv6CP: *IP Control Protocol and* IPv6 *Control Protocol*
3. RARP: *Reverse Address Resolution Protocol*
4. SLIP: *Serial Line* IP

G. *Physical Layer*

1. NIC: *Network Interface Card*
2. Hub/*Switch*

2.6.2 AAA Protocols

Autorization, Authentication and Accounting (AAA) adalah teknologi cerdas untuk mengendalikan akses ke sumber daya perangkat jaringan dengan memverifikasi penggunaan, dan memberikan informasi yang diperlukan untuk layanan kepada penggunanya. *Authentication* menyediakan cara untuk mengidentifikasi pengguna, biasanya dengan memasukkan nama dan *password* yang valid miliki pengguna sebelum akses diberikan. *Authorization* ialah proses

menentukan apakah pengguna memiliki kewenangan untuk mengakses informasi atau jaringan tertentu. Tindakan *Accunting* ialah menghitung sumber daya yang digunakan oleh pengguna, seperti jumlah waktu atau data yang dikirim atau diterima oleh *user* selama melakukan kontrol terhadap jaringan atau sumber yang diaksesnya [3]. Berikut ini contoh protokol yang menggunakan *Autorization, Authentication and Accounting* (AAA) :

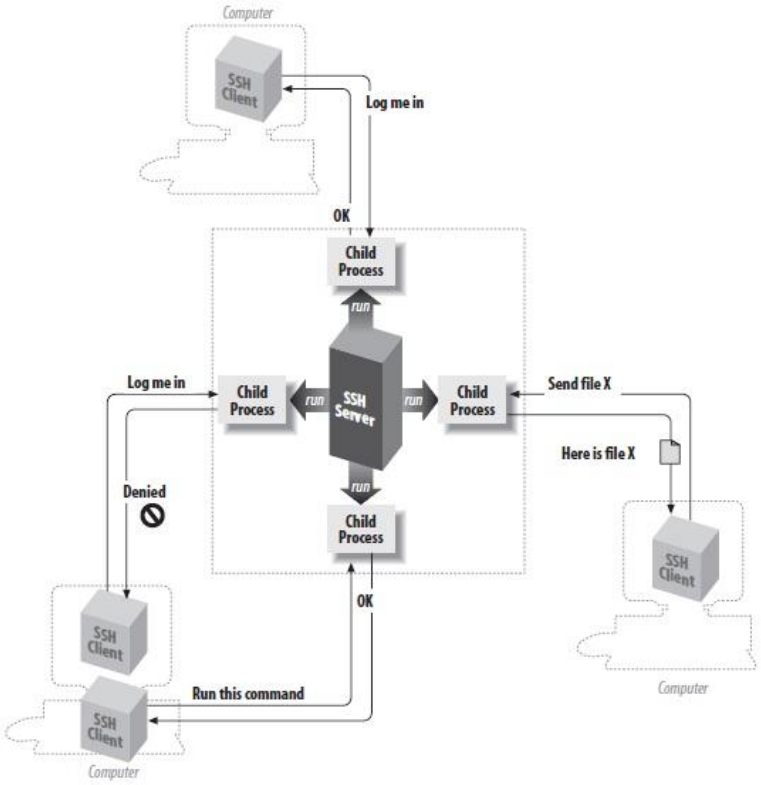
1. Kerberos : *Network Authentication Protocol*
2. RADIUS : *Remote Access Dial In User Service*
3. SSH : *Secure Shell Protocol*

2.7 SSH : *Secure Shell*

SSH (*Secure Shell*) adalah protokol *remote* yang populer berbasis pendekatan yang meminimalisir serangan terhadap suatu jaringan. Setiap kali data dikirimkan kejaringan, SSH secara otomatis meng-enkripsi data atau *command* tersebut. Kemudian ketika data tersebut sampai ke tujuannya, SSH secara otomatis men-dekripsikan data atau *command* tersebut. Hasilnya adalah pengguna dapat bekerja secara normal dan tidak menyadari bahwa komunikasinya telah dienkripsi pada jaringan dengan aman. Metode enkripsi dan algoritma yang digunakan untuk SSH semua didasarkan pada algoritma standar industri seperti 3DES, Blowfish, Twofish, dan AES [4].

SSH memiliki arsitektur *client/server*. Sebuah program server SSH biasanya dipasang dan dijalankan oleh administrator dengan melakukan konfigurasi menerima atau menolak koneksi ke komputer *host.* Administrator kemudian menjalankan SSH-*client* melalui komputer lain untuk mengakses server tersebut agar dapat membuat permintaan dari server SSH [5].

SSH1 dan protokol SSH1 dikembangkan pada tahun 1995 oleh Tatu Ylonen, peneliti Helsinki University of Technology di Finlandia. Setelah jaringan universitas adalah korban dari serangan *password sniffing* awal tahun itu, Ylonen melecut SSH1 untuk dirinya sendiri. Ketika versi beta mulai mendapatkan perhatian, namun, ia menyadari produk keamanannya dapat dimanfaatkan dengan lebih luas **[**5**]**.



Gambar 2.7.1 Arsitektur SSH [5]

Protokol SSH bekerja mencakup autentikasi, enkripsi, dan integritas data yang ditransmisikan melalui jaringan [5].

1. Autentikasi

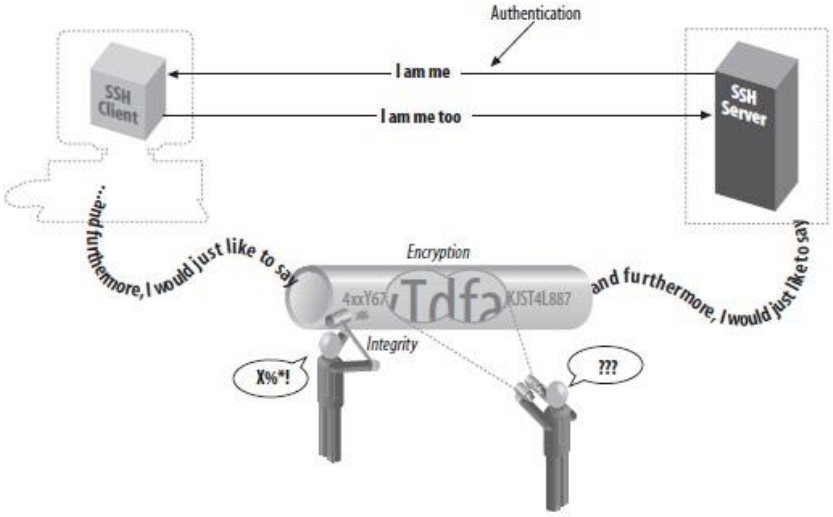
   Jika pengguna mencoba *login* ke akun komputer *remote,* SSH meminta data identitas pengguna seperti, *username* dan *password.* Jika data benar pengguna dapat *login* ke sistem, jika tidak SSH akan menolaknya.

2. Enkripsi

   SSH meng-enkripsi data atau perintah yang dikirimkan dan men-dekripsikannya kepada penerima secara otomatis.

3. Integritas

   Menjamin data atau perintah yang dikirimkan melalui jaringan tidak berubah.



Gambar 2.7.2 SSH Authentication, Encryption, Integrity [5]

2.8 *Remote Access*

Remote access merupakan mekanisme yang biasa digunakan dalam pengendalian suatu perangkat jaringan, dimana administrator dapat dengan mudah mengontrol dan mengawasi komputer *server*, *backup data*, atau aktifitas lainnya yang berhubungan dengan *server* [6].

Pada saat ini banyak media yang dapat digunakan untuk dapat melakukan *remote access* ini seperti komputer/laptop, *smartphone* dan perangkat terkomputerisasi lainnya. Untuk dapat melakukan *remote access* ini diharuskan agar perangkat yang akan terlibat *remote* harus terkoneksi dengan internet atau intranet.

2.9 IP *Address* v4

IP merupakan suatu mekanisme transmisi yang digunakan oleh protokol-protokol TCP/IP, dimana IP bersifat *unreliable, connectionless* dan *datagram delivery service* [7].

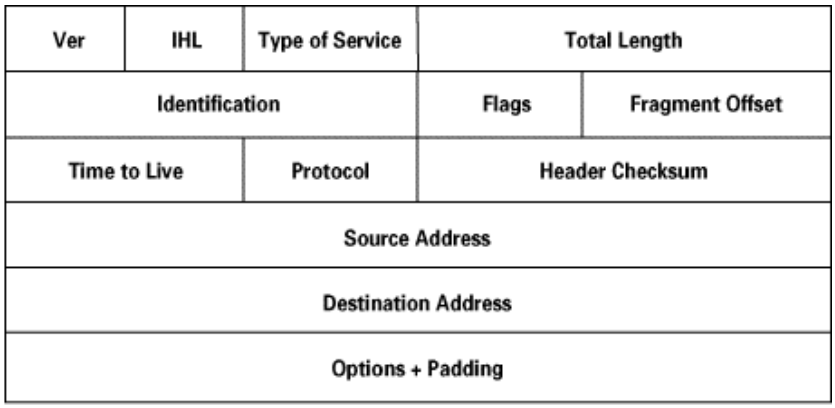
Unreliable berarti bahwa protokol IP tidak menjamin datagram (Paket yang terdapat di dalam IP *layer*) yang dikirim pasti sampai ke tempat tujuan. Protokol IP hanya berusaha sebaik-baiknya agar paket yang dikirim tersebut sampai ke tujuan. Jika dalam perjalanan, paket tersebut mengalami gangguan seperti jalur

putus, kongesti pada *router* atau target *host down*, protokol IP hanya bisa menginformasikan kepada pengirim paket melalui protokol ICMP bahwa terjadi masalah dalam pengiriman paket IP. Jika diinginkan keandalan yang lebih baik, keandalan itu harus disediakan oleh protokol yang berada di atas IP *layer* misalnya TCP dan aplikasi pengguna.

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

Datagram delivery service berarti bahwa setiap paket yang dikirimkan tidak tergantung pada paket data yang lain. Akibatnya jalur yang ditempuh oleh masing-mading paket data bisa jadi berbeda satu dengan yang lainnya.

Alamat IP versi 4 umumnya diekspresikan dalam notasi desimal bertitik (*dotted-decimal notation*), yang dibagi ke dalam empat buah oktet berukuran 8-bit. Dalam beberapa buku referensi, format bentuknya adalah **w.x.y.z**. Karena setiap oktet berukuran 8-bit, maka nilainya berkisar antara 0 hingga 255. Pada gambar di bawah ini ditunjukkan format *header* dari IPv4.



Gambar 2.9.1 IPv4 Header [7]

Informasi yang terdapat pada *header* IPv4 adalah sebagai berikut :

1. *Version* (Ver) : Berisi tentang versi protokol IP yang dipakai.
2. *Information Header Length* (IHL) : Berisi panjang *header* IP bernilai 32 bit.

3. *Type of Service* : Berisi kualitas *service* cara penanganan paket IP.
4. *Total Length* : Total panjang datagram IP dalam ukuran *byte*.
5. *Identification, Flags*, dan *Fragment Offset* : Berisi tentang data yang berhubungan dengan fragmentasi paket.
6. *Time to Live* : Berisi jumlah *router/hop* maksimal yang boleh dilewati paket IP. Setiap kali paket IP melewati *router*, isi *field* akan dikurangi satu. Jika TTL telah habis dan paket belum sampai ke tujuan, paket akan dibuang dan *router* terakhir akan mengirimkan paket ICMP *time exceeded*.
7. *Protocol* : berisi angka yang mengidentifikasikan protokol *layer* atas, yang menggunakan isi data dari paket IP ini.
8. *Header Checksum* : berisi nilai *checksum* yang dihitung dari seluruh *field* dari *header* paket IP. Sebelum dikirimkan, protokol IP terlebih dahulu menghitung *checksum* dari *header* paket IP tersebut untuk nantinya dihitung kembali di sisi penerima. Jika terjadi perbedaan maka paket dianggap rusak dan dibuang.
9. *Source Address* : Alamat asal/sumber.
10. *Destination Address* : Alamat tujuan.
11. *Option* : Mengkodekan pilihan-pilihan yang diminta oleh pengirim seperti *security label*, *source routing*, *record routing*, dan *time stamping*.
12. *Padding* : Digunakan untuk meyakinkan bahwa *header* paket bernilai kelipatan dari 32 bit.

2.9.1 Jenis-Jenis IP Address

Jenis-jenis pada IP *address* membedakan karakteristik dan penggunaannya dalam pengalamatan suatu *client* atau server. Berikut ini dua jenis IP *address* yang digunakan saat ini [7]:

1. IP *Public*

   IP *public* adalah istilah yang digunakan untuk mengidentifikasi host di jaringan internet global.

2. IP *Private*

   IP *Private* merupakan istilah yang dapat digunakan untuk jaringan lokal dan tidak dapat digunakan untuk berkomunikasi dengan dengan *host* di jaringan global (internet).

2.9.2 Kelas-Kelas IP Address

IP address dibagi menjadi lima kelas, A sampai E. IP address yang digunakan secara umum dibagi kedalam 3 kelas, yaitu A sampai C. Sementara 2 kelas lainnya, D dan E dipakai untuk kepentingan khusus. Penggunaan kelas-kelas ini untuk memudahkan pendistribusian IP address ke seluruh dunia [7].

1. Kelas A

   Karakteristik :

   a. Format : 0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh
   b. Bit pertama : 0
   c. Panjang Network ID : 8 bit
   d. Panjang Host ID : 24 bit
   e. Byte pertama : 0 – 127
   f. Jumlah : 126 Kelas A(0 dan 127 *subnetting*)
   g. Range IP : 1.xxx.xxx.xxx sampai 126.xxx.xxx.xxx
   h. Jumlah IP : 16.777.214

2. Kelas B

   Karakteristik :

   a. Format : 10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh
   b. 2 bit pertama : 10
   c. Panjang Network ID : 16 bit
   d. Panjang Host ID : 16 bit
   e. Byte pertama : 128 – 191
   f. Jumlah : 16.384 kelas B
   g. Range IP : 128.0.xxx.xxx sampai 191.155.xxx.xxx
   h. Jumlah IP : 65.535 IP address pada tiap kelas B

3. Kelas C

   Karakteristik :

   a. Format : 110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh
   b. Bit pertama : 110
   c. Panjang Network ID : 24 bit
   d. Panjang Host ID : 8 bit
   e. Byte pertama : 192 – 223
   f. Jumlah : 2.097.152 kelas C
   g. Range IP : 192.0.0.xxx sampai 223.255.255.xxx
   h. Jumlah IP : 254 IP address pada tiap kelas C

4. Kelas D

   Karakteristik :

   a. Format:1110mmmm.mmmmmmmm.mmmmmmmm.mmmmmmmm
   b. 4 bit pertama : 1110
   c. Bit Multicast : 28 bit
   d. Byte Inisial : 8 bit
   e. Byte pertama : 224-247
   f. Deskripsi : Kelas D adalah ruang alamat Multicast (RFC 1112)

   IP kelas D digunakan sebagai alamat multicast yaitu sejumlah komputer memakai yang memakai aplikasi bersama. 4 bit pertama IP address kelas D di set 1110. Dalam multicasting tidak dikenal network bit dan host bit.

5. Kelas E

   Karakteristik :

   a. Format : 1111eee.eeeeeeee.eeeeeeee.eeeeeeee
   b. 4 bit pertama : 1111
   c. Bit Multicast : 28 bit
   d. Byte Inisial : 248-255
   e. Deskripsi : Kelas E adalah ruang alamat untuk keperluan eksperimental.

2.10 *Subnetting*

Konsep *subnetting* dari IP address merupakan teknik yang umum digunakan di internet untuk mengefisiensikan alokasi IP address dalam sebuah jaringan supaya bisa memaksimalkan penggunaan IP address [7].

Tujuan lain yang tidak kalah pentinganya dari subnetting adalah untuk mengurangi tingkat kongesti dalam suatu *network*. Untuk menghindari terjadinya kongesti akibat terlalu banyak host dalam suatu *physical network,* dilakukan segmentasi jaringan.

Esensi dari *subnetting* adalah "memindahkan" garis pemisah antara bagian *network* dan bagian host dari suatu IP address. Beberapa bit dari bagian host dialokasikan menjadi bit tambahan pada bagian *network*. Address suatu *network* menurut struktur baku dipecah menjadi beberapa sub-network. Cara ini menciptakan sejumlah *network* tambahan dengan mengurangi jumlah maksimum *host* yang ada dalam tiap *network* tersebut.

2.11 Mikrotik RouterOS

Mikrotik RouterOS adalah perangkat lunak *routing* yang populer dan berkembang sangat pesat. Apabila dikombinasikan dengan perangkat keras dengan spesifikasi yang kuat, RouterOS diyakini dapat melampaui router yang saat ini tersedia di pasaran [8].

RouterOS dapat bekerja pada beberapa jenis perangkat keras yang berbeda. Mikrotik menghasilkan perangkat keras mereka sendiri berdasarkan pendekatan *single board* yang disebut dengan Routerboard. Routerboard hadir dengan spesifikasi yang berbeda-beda, seperti nomor port Ethernet, slot nirkabel, konfigurasi pada memori yang digunakan serta desain perangkat keras.



Gambar 2.11.1 Tampilan Mikrotik RouterOS 5.20

2.12 BBSSH

BBSSH adalah adalah sebuah aplikasi SSH dan telnet *client* untuk perangkat Blackberry. Aplikasi SSH *client* ini memiliki fitur yang cukup praktis untuk digunakan seperti disediakannya fitur tombol keyboard, dan macro untuk membuat perintah sederhana yang akan digunakan untuk mengakses suatu jaringan [9].

Aplikasi ini *multitasking* sehingga apabila digunakan tidak akan mengganggu fungsional *smartphone* lainnya seperti telepon, SMS, email, dan lainnya. Aplikasi ini bersifat *free* sehingga pengguna tidak perlu memikirkan lisensi dan batas waktu dalam menggunakannya.



Gambar 2.12.1 Penggunaan BBSSH dan Fungsi Macro