BAB II
TINJAUAN PUSTAKA

2.1 Jaringan Komputer

Merupakan hubungan dari sejumlah perangkat yang dapat saling berkomunikasi satu sama lain. Pada jaringan komputer terdapat dua buah komputer atau perangkat yang saling terhubung satu sama lain dan terjadi proses komunikasi dan transfer paket data di dalamnya.

Berdasarkan klasifikasinya, jaringan komputer dibagi menjadi :

1. Cakupan area geografis
2. Topologi jaringan
3. Arsitektur Komputer

2.1.1 Cakupan Area Geografis

Berdasarkan cakupan area goegrafis, jaringan komputer dibagi menjadi :

1. *Local Area Network* (LAN)

   LAN digunakan untuk menghubungkan komputer yang berada didalam suatu area kecil, misal didalam gedung kantor atau kampus. Jarak antara komputer yang dihubungkan biasa mencapai 5 sampai 10Km. suatu LAN biasanya bekerja pada kecepatan 10 Mbpa sampai 100 Mbps.
2. *Metropolitan Area Network* (MAN)

   MAN merupakan suatu jaringan yang cakupannya meliputi suatu kota. MAN menghubungkan LAN-LAN yang lokasinya berjahuan. Jangkauan MAN bias mencapai 10Km sampai beberapa ratus Km. MAN biasanya bekerja pada kecepatan 1,5 sampai 150 Mbps.
3. *Wide Area Network* (WAN)

   WAN dirancang untuk menghubungkan komputer-komputer yang terletak pada suatu cakupan geografis yang luas, seperti hubungan dari satu kota ke kota lain di suatu Negara. Cakupan WAN bias meliputi 100Km sampai 1,000 Km, dan kecepatan antar kota bias bervariasi antara 1,5 Mbps sampai 2,4

Gbps. Dalam WAN, biaya untuk transmisi sangant tinggi, dan biasanya jaringan WAN dimiliki dan di operasikan sebagai suatu jaringan publik.

2.1.2 Topologi Jaringan Komputer

Topologi jaringan adalah gambaran perencanaan hubungan antarkomputer dalam LAN yang umumnya menggunakan kabel (sebagai media transmisi), dengan konektor, *ethernet card*, dan perangkat pendukung lainnya. Ada beberapa jenis topologi yang terdapat pada jaringan komputer, seperti:

1. Topologi Bus

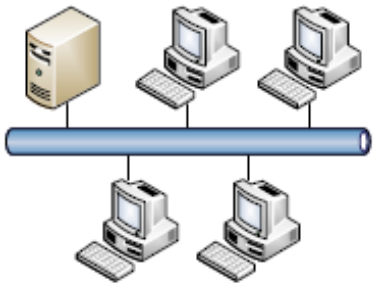
Topologi bus merupakan koneksi bertipe *multipoint,* sebuah bentang kabel tunggal yang panjang akan bertindak sebagai *backbone* yang akan menghubungkan semua perangkat dalam jaringan. *Node-node* terhubung ke kabel *Bus* melalui *drop line* dan *tap. Drop line* adalah suatu konektor yang berjalan antara perangkat dan kabel utama. *Tap* adalah konektor yang juga tersambung pada kabel utama (terhubung langsung pada inti logam kabel).

Kelebihan dari topologi *Bus :*

- *Instalasi* mudah. Kabel *backbone* dapat diletakan ditempat manapun yang paling efisien, kemudian dihubungkan pada *node-node* melalui *drop line.*
- Penggunaan kabel lebih sedikit.

Kekurangan topologi *Bus*:

- *Backbone* rusak maka semua jaringan lumpuh atau tidak berfungsi.
  Sangat sulit untuk mengindentifikasi permasalahan jika jaringan sedang rusak.



Gambar II-1 Topologi Bus

2. Topologi Star

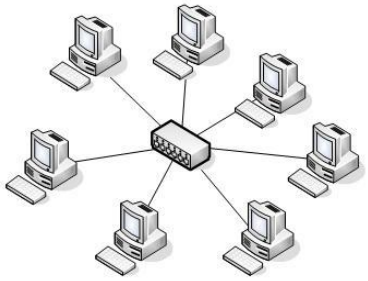
Topologi star adalah topologi yang memiliki pusat berupa *hub* dan *switch* yang berfungsi untuk menghubungkan dan meneruskan pengiriman data antar perangkat.

Kelebihan topologi *Star* :

- Satu *link* yang rusak tidak akan mempengaruhi *link* yang lain.
- Mudah dalam hal *installasi* dan *konfigurasi.*
- Penambahan dan pengurangan perangkat hanya melibatkan perangkat itu sendiri

Kekurangan topologi *Star*:

- Membutuhkan lebih banyak kabel.
- Jika pusat penghubung rusak atau mati semua perangkat yang terhubung tidak dapat melakukan pengiriman atau pengambilan data.



Gambar II-2 Topologi Star

3. Topologi Ring

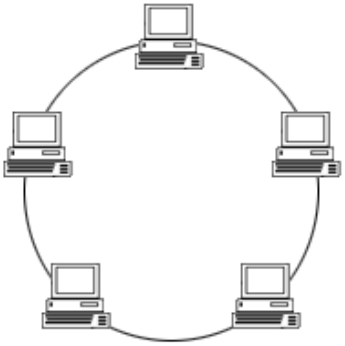
Topologi *Ring* adalah topologi yang setiap perangkat terhubung secara seri dengan yang lain sehingga membentuk satu lingkaran yang tertutup (*loop*).

Kelebihan Topologi *Ring*:

- *Installasi* dan *konfigurasi* relative mudah.
- Didukung oleh banyak perangkat keras dan perangkat lunak

Kekurangan Topologi *Ring*:

- Sulit untuk dikembangkan keselakal jaringan yang besar.
  Jika jaringan utama rusak, maka keseluruhan *segment* akan rusak juga.



Gambar II-3 Topologi Ring

4. Topologi Mesh

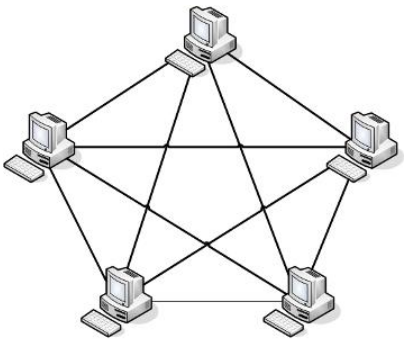
Setiap perangkat terhubung secara *dedicade point-to-point* kesemua perangkat. Dan beban koneksi satu *link* tidak akan menggang *link* lainnya

Kelebihan topologi *mesh:*

- *Dedicade link* menjamin bahwa setiap koneksi hanya membawa beban datanya sendiri. Hal ini menghilangkan masalah *traffic* yang terjadi jika *link* dibagi.
- Kerusakan satu *link* tidak akan menggangu *link* lainnya.
- Data aman karena hanya ada pengirim dan penerima, tidak bisa di *intervensi* oleh user lain.

Kekurangan topologi *mesh*:

- Butuh banyak kabel dan butuh banyak port.
- Mahal dan sulit saat *installasi*.



Gambar II-4 Topologi Mesh

2.1.3 Arsitektur Jaringan Komputer

Berdasarkan arsitekturnya jaringan dibagi menjadi:

1. *Client Server*

   Client Server adalah jaringan komputer yang salah satu komputer difungsikan sebagai server atau komputer yang memberikan pelayanan kepada komputer lain. Server melayani komputer-komputer lain yang disebut client. Layanan yang diberikan bisa berupa akses web, e-mail, file atau yang lainya. *Client Server* banyak dipakai pada *Internet.* Namun LAN atau jaringan lainpun bisa mengimplementasikan *cleint server*.

2. *Peer to Peer*

   Peer-to-peer adalah jaringan komputer dimana setiap komputer bisa menjadi server sekaligus client. Setiap komputer dapat menerima dan memberikan akses dari satu komputer ke komputer lain.

2.2 Protokol Jaringan

Pada jaringan komputer, komunikasi terjadi antara *entitas* dalam sistem yang berbeda. *Entitas* adalah segala sesuatu yang mampu mengirim dan menerima informasi. Namun dua *entitas* tadak dapat langsung mengirim aliran bit satu sama lain, juga tidak dapat langsung saling mengerti. Agar komunikasi dapat dilakukan, *entitas-entitas* tersebut harus memiliki suatu protokol.

Protokol adalah kumpulan aturan yang mengatur komunikasi data. Protokol mengindentifikasi apa itu komunikasi, bagaimana cara berkomunikasi, serta kapan komunikasi dapat dilakukan.

Elemen kunci dari protokol adalah sebagai berikut[1]:

1. *Syntax*

   Istilah *syntax* merupakan struktur atau format data yang digunakan untuk mengkodekan sinyal.

2. *Semantics*

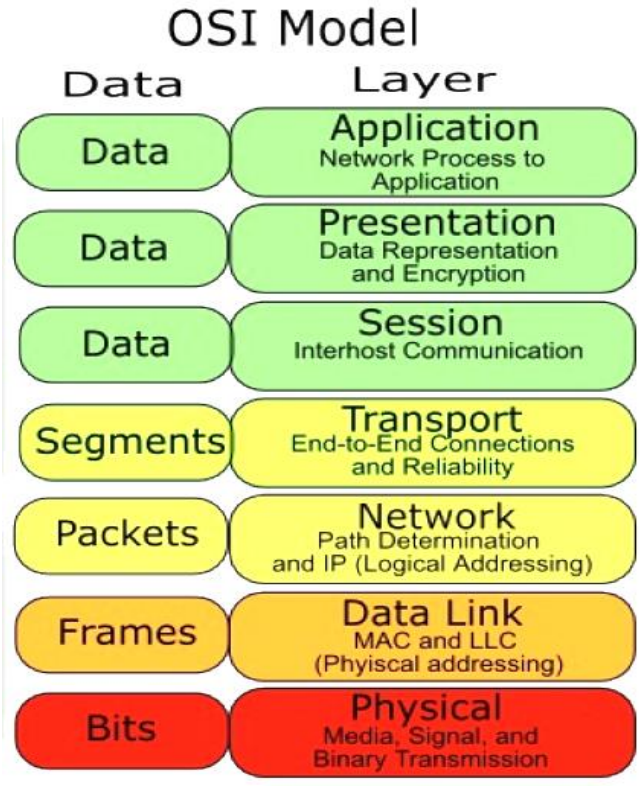
   Semantics digunakan untuk mengetahui maksut dari informasi yang dikirim dan mengoreksi kesalahan yang terjadi dari informasi

3. *Timing*

Istilah *Timing* mengacu pada dua karakteristik kapan data dikirim dan seberapa cepat data tersebut dapat dikirim.

2.3 Open System Interconnection (OSI)

Open System Interconnection (OSI) adalah kumpulan protokol yang memungkinkan dua sistem yang berbeda dapat berkomunikasi tanpa memperhatikan arsitektur yang mendasari sistem tersebut. Tujuan OSI model adalah untuk menunjukan bagai mana cara untuk memfasilitasi dua sistem yang berbeda tanpa memerlukan perubahan logika pada *hardware* dan *software*. OSI model bukan suatu protocol melainkan model untuk memahami dan merancang arsitektur jaringan yang *fleksibel*, kokoh dan mudah di operasikan. OSI model merupakan *framwork* berlapis untuk merancang sistem jaringan yang memungkinakan komunikasi antara semua jenis komputer[1].



Gambar II-5 Lapisan OSI Model

Berikut penjelasan fungsi dari gambar model OSI diatas :

1. *Application layer* (Lapisan Aplikasi)

   Application Layer bertugas untuk menyediakan layanan pada pengguna. Layanan ini memungkinkan pengguna, baik manusia atau *software* untuk

mengakses jaringan. Layer ini menyediakan user *interface* dan dukungan untuk layanan-layanan seperti e-mail, akses remote file dan layanan-layanan lainnya.

2. *Presentation layer* (Lapisan Presentasi)

Presentation Layer berhubungan dengan format data yang digunakan antara dua sistem yang saling bertukar data. *Presentation Layer* memiliki tugas utama yaitu :

- Translasi yang berguna untuk menerjemahkan kode data dari setiap sistem yang berbeda-beda
- *Enkripsi* yang berguna untuk mengubah informasi asli yang akan dipertukarkan menjadi bentuk lain agar aman ketika melalui jalur pengiriman.
- Kompresi yang berguna untuk mengurangi jumlah bit pada informasi yang akan dipertukarkan.

3. *Session Layer* (Lapisan Sesi)

Session Layer bertugas untuk mengelola dialog dan *sinkronisasi.* Tanggung jawab dari *Session Layer* adalah sebagai *Dialog Control* yaitu lapisan sesi yang memungkinkan kedua sistem untuk membangung dialog serta tanggung jawab untuk *Synchronization* pada interaksi antara sistem komunikasi.

4. *Transport Layer* (Lapsisan Transport)

Transport layer bertugas untuk mengirim pesan dari satu proses ke proses yang lain. Proses adalah program aplikasi yang berjalan pada host. Tugas lain *Transport Layer* adalah:

- *Service-point addressing* karena sering menjalankan beberapa program pada waktu yang sama, maka pengirim *source-to-destination* tidak hanya dari satu komputer ke komputer lain, tapi juga dari satu *spesificprocess* pada komputer lain.
- *Segment and reasembly*. Berguna untuk memastikan seluruh pesan yang sampai dibagian penerima dalam keadaan utuh dan sesuai urutan dan melakukan *indentifikasi* serta pergantian paket jika terjadi kehilangan pada saat proses pengiriman.

- *Connection control*. Lapisan *transport* bisa berupa *connectionless* atau *connection-oriented, Transport layer* secara *connectionless* memerlukan setiap segment sebagai paket yang individu dan mengirimnya ke *transport layer* pada tujuan. *Transport layer connection-oriented* akan membangun koneksi terlebih dahulu dengan *transport layer* pada tujuan sebelum paket dikirim. Dan setelah semua data terkirim, koneksi akan dipututskan.
- *Flow Control* dilakukan di *end-to-end,* bukan di *single link*.
- *Error Control* memastikan seluh pesan sampai pada lapisan *transport* di penerima tanpa ada masalah. *Error Control* dilakukan pada proses ke proses, bukan di *single link.*

5. *Netwok Layer* (Lapisan Jaringan)

Network layer bertugas untuk mengirimkan paket-paket individu dari *host sender* ke *host receiver*, sekalipun melewati banyak jaringan (*link*). Tugas lain dari layer ini adalah:

- *Logical addressing,* network layer akan menambahkan header yang berisi IP sumber dan tujuan pada paket yang datang dari layer diatasnya.
- *Routing,* merupakan mekanisme untuk memilih atau mengerahkan paket ketujuan akhir paket tersebut. Perangkat yang melakukan fungsi tersebut adalah *Router*.

6. *Data Link Layer* (Lapisan Data link)

Data Link layer bertugas dalam perpindahan *frame* dari satu *hop* (mode) ke *hop* yang selanjutnya. Tugas lain dari layer ini adalah:

- *Framing,* aliran bit yang diterima akan dibagikan menjadi *frame-frame.*
- *Physical addressing,* data link layer akan memberikan header pada *frame* untuk mendefenisikan *sender* dan *receiver* dari *frame* tersebut.
- *Flow control,* rate data di-produce akan di sesuaikan dengan rate yang bisa diterima oleh *receiver.* Hal ini dilakukan agar *receiver* tidak kewalahan saat menerima data.
- *Error control* untuk mendeteksi dan mengirim ulang frame yang rusak. *Error control* akan mengetahui jika terjadi duplikat pada *frame.*

- *Access control* jika terdapat dua perangkat atau lebih terhubung pada link yang sama, protokol data link layer akan menentukan perangkat mana yang memiliki kontrol atas link tersebut pada waktu tertentu.

7. *Physical Layer* (Lapisan Fisik)

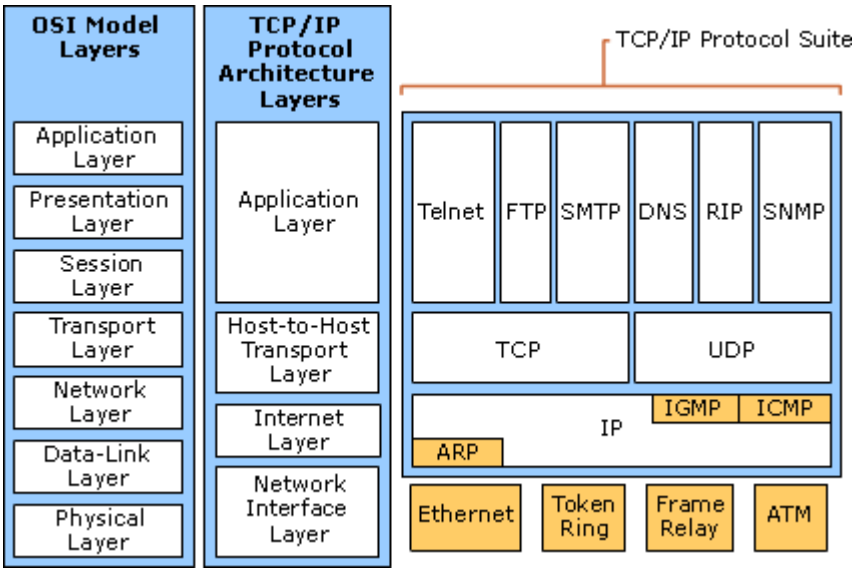
Physical Layer bertugas untuk perpindahan bit-bit tunggal dari satu hop (node) ke hop yang selanjutnya. Layer ini juga menentukan prosedure dan fungsi yang harus dijalankan oleh perangkat fisik dan antarmuka agar transmisi dapat dilakukan. *Physical Layer* juga mengelola hal-hal berikut:

- Karakteristik fisik dari antarmuka dan media perantara.
- Representasi bit data pada layar ini terdiri dari aliran bit (0 atau 1) tanpa *interpretasi*. Agar dapat ditransmisikan, bit-bit ini harus di-*encode* menjadi sinyal listrik atau optik.
- Data rate atau *transmission* rate adalah jumlah bit yang dikirim setiap satu waktu.
- *Sinkronisasi* bit, bit level dan bit rate *sender* dan *receiver* harus sama.
- *Line configuration* layer ini juga memperhatikan koneksi perangkat ke media. Pada konfigurasi point-to-point, koneksinya *dedicated link*. Pada *konfigurasi multipoint*, link di-share pada beberapa perangkat.
- Topologi fisik yaitu menggambarkan secara fisik atau nyata bagaimana perangkat-perangkat terhubung satu sama lain hingga menjadi suatu jaringan.
- *Transmission mode* menentukan arah transmisi dari perangkat yang sedang melakukan pertukaran data. *Simplex* yaitu hanya satu perangkat yang bisa mengirimkan data dan yang lainnya hanya menerima. *Half-Duplex* yaitu dua perangkat bisa mengirim dan menerima data tapi tidak dalam waktu yang bersamaan. *Full-Duplex* yaitu setiap perangkat bisa mengirim dan menerima data dalam waktu yang bersamaan.

2.4 TCP/IP Protocol Suite

TCP/IP protocol suite dikembangkan sebelum model OSI. Namun lapisan-lapisan pada TCP/IP tidak sama dengan lapisan-lapisan yang dimiliki oleh OSI.

Protocol TCP/IP hanya diabuat atas lima lapisan, yaitu: *pyshical, data link, network, transport* dan *application.*



Gambar II-6 Lapisan TCP/IP

Berikut penjelasan dari setiap lapisan protocol TCP/IP :

1. *Aplication layer* (Lapisan Aplikasi)

   Lapisan aplikasi pada TCP/IP setara dengan tiga lapisan yang terdapat pada model OSI. Bentuk data pada lapisan ini biasa disebut dengan *message.* Komunikasi pada lapisan ini juga sama seperti lapisan transport yaitu *end-to-end.* Beberapa protocol yang ada pada lapisan ini sebagai berikut:

   - HTTP (*Hyper Text Transfer Protocol*) yang digunakan untuk layanan web.
   - Telnet yang berfungsi untuk melakukan remote pada suatu host
   - FTP (*File Transfer Protocol*) yang digunakan untuk keperluan *file sharing.*

2. *Transport* Layer (Lapisan Transport)

   Terdapat perbedaan utama pada lapisan jaringan dan lapisan transport. Setiap node memerlukan lapisan transport. Dilapaisan ini pula terdapat protokol yang bisa digunakan untuk pengiriman data yaitu *User Datagram Protocol* (UDP) dan *Transmission Control Protocol* (TCP).

3. *Internet Layer* (Lapisan Internet)

   Berfungsi untuk menyediakan *Routing* dan pembuatan paket menggunakan teknik *encaptulation*. *Internet layer* memiliki tugas utama untuk memilih

rute dalam sebuah jaringan. Selain itu layer ini juga bertugas untuk melakukan *paket swictching*.

4. *Network Layer* (Lapisan jaringan)

   Berfungsi untuk menyediakan *frame-frame* data yang akan dikirim kemedia jaringan. Layer ini bertugas mengatur semua hal yang diperlukan oleh sebuah paket IP.

2.5 Keamanan Jaringan (*Network Security*)

Keamanan jaringan merupakan hal yang sangat penting untuk diperhatikan dalam sebuah jaringan komputer (*Network Securty*). Adanya keamanan jaringan maka resiko yang tidak diinginkan akan dapat dikurangi, dengan demikian pada *user* atau pengguna akan merasa aman saat bekerja di jaringan komputer yang mereka gunakan.

Sebuah jaringan dengan desain dasar yang aman memerlukan beberapa penerapan aturan dasar yang sederhana yang perlu disesuaikan dengan kontek yang berbeda, seperti berikut :

- Menutup port IP yang tidak terpakai.
- Memusatkan titik *control traffic.*
- Periksa semua jalur akses dan desain multilayer dalam kasus jaringan yang kompleks.

Selain itu, keamanan jaringan juga mempunyai tujuan yang dapat membuat jaringan lebih ditingkatkan lagi, yaitu :

1. *Confidentiality*

   Adanya data-data yang penting yang biasanya tidak boleh diakses oleh seseorang, sehingga dilakukan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Biasanya *confidentiality* ini berhubungan dengan informasi yang diberikan kepihak lain.

2. *Integrity*

   Pesan yang disampaikan ke penerima tetap orisinil yang tidak diragukan keasliannya, tidak dimodifikasi selama dalam pengiriman sumber ke penerimanaya.

3. *Availability*

Dimana *user* yang mempunyai hak akses diberikan akses tepat pada waktunya, biasanya ini berhubungan dengan ketersedian informasi atau data ketika dibutuhkan.

Keamanan jaringan komputer sendiri bertujuan untuk mengantisipasi resiko pada jaringan komputer, berupa bentuk ancaman fisik maupun logik, baik langsung (*direct*) ataupun tidak langsung (*indirect*) menggangu aktivitas yang sedang berlangsung dalam jaringan komputer. Secara umum, terdapat 3 hal dalam konsep keamanan jaringan, yakni :

1. Resiko (*Risk*): resiko disini adalah untuk menyatakan besarnya kemungkinan gangguan yang muncul terhadap jaringan.
2. Ancaman (*Threat*): ancaman disini merupakan kemungkinana gangguan yang muncul terhadap jaringan.
3. Kerapuhan sistem (*Vulnerability*): ancaman disini menyatakan kelemahan-kelemahan pada sistem yang memungkinkan terjadinya gangguan.

2.6 Intrusion Detection System (IDS)

IDSmerupakan sistem untuk mendeteksi adanya *intrusion* yang dilakukan oleh *intruder* atau penyusup di dalam jaringan. IDS sendiri sangat mirip seperti alarm, apabila IDS mencatat adanya suatu serangan atau gangguan dalam jaringan, maka IDS akan memperingati administrator jaringan tersebut. IDS (I*ntrusion Detection System*) dapat didefenisikan sebagai kegiatan yang bersifat *anomaly*, *incorrect*, *inappropriate* yang terjadi dijaringan atau host. Dan IDS sendiri adalah sistem keamanan yang bekerja bersama *Firewall* untuk mengatasi *Intrusion*[2].

Berikut beberapa komponen yang terdapat pada IDS [4]:

1. *Sensor* : yang dapat mengenali adanya *security event.*
2. *Console* : yang dapat memonitor event, *alert* dan mengontrol sensor
3. *Central Engine* : yang mana berguna untuk menyimpan *events logged* yang dilakukan oleh sensor kedalam database dan menggunakan aturan-aturan keamanan yang berguna untuk menagani event yang terjadi.

Apabila ada aktivitas yang dianggap mencurigakan di dalam jaringan makan IDS akan mendeteksi dan mencatat semua aktivitas yang mencurigakan tersebut.

Namun IDS ini tidak dapat melakukan tindakan atau pencegahan jika terjadi serangan atau penyususpan didalam jaringan.

Namun IDS mempunyai peran yang cukup membantu dalam hal yang berkaitan dengan keamanan jaringanan, diantaranya :

a. Secara aktif mengamati segala macam kegiatan yang mencurigakan.
b. Memeriksa *audit logs* dengan sangat cermat dan seksama.
c. Mengirim *alert* kepada administrator saat adanya serangan yang terdeteksi.
d. Memberikan laporan segala macam kerentanan yang ditemukan.

Namun kembali lagi kepada kemampuan IDS yang terbatas, yang hanya bisa mencatat dan memberikan laporan kepada administrator, karena IDS tidak dapat menghentikan serangan tersebut.

Dilihat dari kemampuan mendeteksi serangan dalam jaringan, maka IDS dibagi menjadi dua, yaitu [3]:

1. Network-Based IDS (NIDS)

Network-Based Intrusion Detection System (NIDS) akan melakukan *capture paket data* yang masuk pada jaringan LAN atau Wireless dan mengumpulkan paket-paket data tersebut, serta melakukan analisa terhadapt paket-paket tersebut apakah paket normal atau paket serangan.

2. Host-Based IDS (HIDS)

Host-based Intrusinon detection system (HIDS) hanya melakukan pemantauan pada perangkat komputer tertentu dalam jaringan. IDS dapat melihat kedalam sistem dan aplikasi file log untuk mendeteksi aktivitas penyusup. HIDS hanya akan berkerja apabila terjadi serangan dan akan memberikan laporan atau peringakatan kepada administrator secara *real time.*

2.7 Snort

Snort merupakan *open source intrusion detection system* (IDS) yang bisa di konfigurasi sebagai *intrusion prevention system* (IDS) untuk pemantauan dan pencegahan pada keamanan komputer.

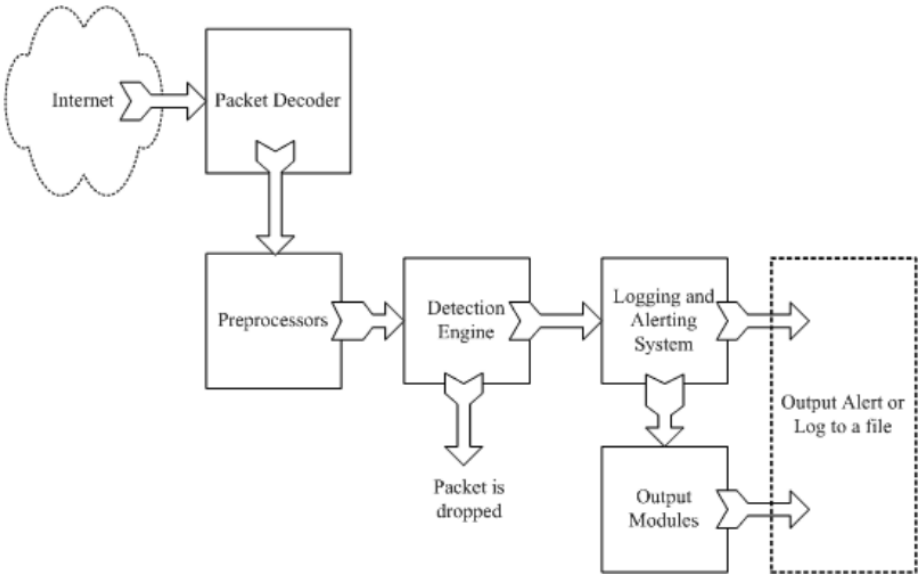
Ketika bekerja sebagai IDS, Snort dapat mendeteksi serangan atau paket data yang masuk kedalam jaringan komputer dan memperingatkan administrator jaringan untuk mengambil tindakan pencegahan. Jika kita menngkonfigurasi Snort

sebagai IPS maka Snort dapat mencegah serangan atau paket data yang berbahaya yang masuk kedalam jaringan, dengan cara memodifikasi IP Table.

Snort secara logis dibagi menjadi beberapa komponen. Komponen-komponen ini bekerja sama untuk mendeteksi serangan tertentu dan untuk mengasilkan *output* dengan format yang dibutuhkan pada *system detection*[4].

Berikut beberapa komponen utama pada Snort :

1. Paket decoder
2. Preprocessors
3. Detection Engine
4. Logging and Alerting System
5. Output modules



Gambar II-7 Komponen Snort

2.7.1 Paket Decoder

Paket Decoder berfungsi untuk mengambil paket dari berbagai jenis *network interface* dan mempersiapkan paket yang akan di *preprocessed* atau dikirim ke *Detection Engine*.

2.7.2 Preprocessors

Preprocessor adalah komponen atau plug-in yang dapat digunakan dengan Snort untuk mengatur atau memodifikasi paket data sebelum *detection engine*

melakukan beberapa operasi untuk mengetahui apakah paket yang digunakan oleh penyusup. Beberapa preprocessor juga melakukan deteksi dengan mencari anomaly dalam header paket dan menghasilkan *alert*. *Preprocessor* sangat penting untuk setiap IDS untuk mempersiapkan paket data yang akan dianalisa terhadapat aturan dalam *detection engine*.

2.7.3 Detection Engine

Detection Engine adalah bagian paling penting dari Snort. *Detection Engine* bertanggung jawab untuk mendeteksi jika ada aktivitas *intrusi* dalam sebuah paket. *Detection Engine* menggunakan *rule* Snort. Untuk tujuan ini, rule dibaca dengan struktur data internal atau dimana mereka cocok dengan semua paket. Jika sebuah paket cocok dengan rule apapun, maka tindakan yang tepat akan dilakukan atau diambil tetapi jika tidak paket akan dibuang.

Detection Engine adalah *time-critical* bagian dari Snort. Tergantung pada seberapa kuat mesin adan berapa banyak aturan telah ditetapkan, mungkin diperlukan jumlah waktu yang berbeda untuk merespon paket yang berbeda, jika lalulintas (*traffic*) di jaringan terlalu tinggi, maka ketika Snort NIDS bekerja dalam model ini, mungkin ada beberapa paket yang di drop dan mungkin tidak mendapatkan real-time respone yang benar.

Beberapa faktor beban pada *detection engine* :

- Jumlah rule
- Kekuatan mesin dalam menjalankan Snort
- Kecepatan internet bu yang dugunakan dalam mesin Snort.
- Load pada jaringan.

2.7.4 Logging and Alerting System

Tergantung pada apa yang *detection engine* temukan dalam sebuah paket, paket digunakan untuk mencatat aktivitas atau menghasilkan peringatan. Nantinya log akan disimpan dalam bentuk file teks sederhana.

2.7.5 Output Modules

Output module atau plug-in dapat melakukan operasi yang berbeda tergantung pada administrator dalam menyimpan output yang dihasilkan oleh *logging* dan *system alert* dari Snort. Pada dasarnya modile ini mengontrol jenis putput yang dihasilkan oleh logging dan memperingatkan system.

2.8 Basic Analysis and Security Engine (BASE)

BASE merupakan *interface* yang akan digunakan untuk menganalisa *output* dari Snort. BASE bekerja dengan menggunakan *query* pada *log database* Snort yang akan disimpan kedalam *database mysql server*. Kemudian akan menampilkan kedalam bentuk web sehingga *log database* tersebut mudah untuk di analisa.

2.9 Sistem Operasi

Suatu program yang mengontrol eksekusi program aplikasi dan berfungsi sebagai media *interface* antara pengguna komputer dengan hardware komputer. System operasi memiliki tiga tujuan :

1. Kemudahan : sistem operasi membuat komputer menjadi lebih mudah dipakai
2. Efesiensi : sistem operasi memungkinkan sumber daya system komputer untuk digunakan dengan cara yang efesien
3. Kemampuan berkembang : sistem operasi harus disusun sedemikian rupa sehingga memungkinkan pengambang yang efektif, pengujian, dan penerapan fungsi-fungsi system yang baru tanpa menggangu layanan yang telah ada.

2.10 Linux

Linux awalnya merupakan varian dari UNIX untuk arsitektur IBM. Versi awal dituliskan oleh Linux Torvalds, seorang mahasiswa ilmu komputer dari Firlandia. Torvalds memposting versi awal Linux di Internet tahun 1991. Karena Linux gratis dan sumber kodenya tersedia, menjadi alternative awal untuk workstation UNIX seperti yang ditawarkan oleh Sun Microsystem, Digital Equipment Corp (sekarang menjadi Compaq), dan Silicon Graphich.

2.10.1 Ubuntu

Ubuntu diambil dari Bahasa Afrika kuno yang berarti *Humanity to Others* atau rasa peri kemanusiaan terhadapat sesama. Tujuan dari distribusi Linux Ubuntu adalah membawa semangat yang terkandung didalam Ubuntu ke dunia perangkat lunak. Ubuntu merupakan varian atau turunan dari Debian, yang merupakan salah satu distro Linux tertua selain Red Hat dan Slackware.

Ubuntu dibentuk berdasarkan gagasan yang terdapat dalam filosofi Ubuntu, yaitu perangkat lunak harus tersedia secara gratis dan tidak ada biaya lisensi, perangkat lunak harus dapat digunakan dalam Bahasa lokal masing-masing dan untuk orang-orang yang mempunyai keterbatasan fisik, serta bersifat serta bersifat open source sehingga pengguna memiliki kebebasan untuk mengubahnya sesuai dengan kebutuhan komputasi mereka.

Kebebasan inilah yang membuat Ubuntu berbeda dari pesaingnya misalnya Microsoft Windows yang bersifat *proprietary* atau berlisensi. Ubuntu dapat diperoleh secara gratis apabila anda memintanya langsung kepada Canonical Ltd. Selain itu, Ubuntu juga memberikan kebebasan untuk memodifikasi Ubuntu agar menjadi distro Linux yang di inginkan. Bahkan, dapat menamai sendiri versi Ubuntu hasil modifikasi tersebut.

2.10.2 Rilis Ubuntu

Setiap rilis Ubuntu memiliki keunikan pada nama kode dan nomor versi yang dikeluarkan. Misalnya nama diambil dari nama binatang dan diikuti dengan nomor versi berdasarkan tahun dan bulan dari rilis. Setiap tahun umumnya akan ada 2 rilis Ubuntu, biasanya pada bulan April dan Oktober. Edisi Ubuntu biasanya di rilis sedikitnya dalam 3 edisi yaitu *Desktop, Alternate* dan *Server*. Perbedaan mendasar ketiganya adalah kegunaan dan cara instalasi. Edisi Desktop digunakan untuk komputer personal dengan instalasi mode grafis. Ubuntu Alternate juga digunakan untuk komputer personal namun instalasi menggunakan mode teks. Ubuntu Server digunakan untuk komputer server dengan instalasi teks. Berikut versi-versi Ubuntu dari awal rilis sampai sekarang :

Versi	Kode nama	Tanggal Perilisan	Didukung sampai	
			Desktop	Server
4.10	Warty Warthog	20-10-2004	2006-04-30	
5.04	Hoary Hedgehog	08-04-2005	2006-10-31	
5.10	Breezy Badger	13-10-2005	2007-04-13	
6.06 LTS	Dapper Drake	01-06-2006	2009-07-14	2011-06-01
6.10	Edgy Eft	26-10-2006	2008-04-25	
7.04	Feisty Fawn	19-04-2007	2008-10-19	
7.10	Gutsy Gibbon	08-10-2007	2009-04-18	
8.04 LTS	Hardy Heron	24-04-2008	2011-05-12	2013-04
8.10	Intrepid Ibex	30-10-2008	2010-04-30	
9.04	Jaunty Jackalope	23-04-2009	2010-10-23	
9.10	Karmic Koala	29-10-2009	2011-04-30	
10.04 LTS	Lucid Lynx	29-04-2010	2013-04	2015-04
10.10	Maverick Meerkat	10-10-2010	2012-04-10	
11.04	Natty Narwhal	28-04-2011	2012-10-28	
11.10	Oneiric Ocelot	13-10-2011	2013-05-09	
12.04 LTS	Precise Pangolin	26-04-2012	2017-04	
12.10	Quantal Quetzal	18-10-2012	2014-05-16	
13.04	Raring Ringtail	25-04-2013	2014-01-27	
13.10	Saucy Salamander	17-10-2013	2014-07-17	
14.04 LTS	Trusty Tahr	17-04-2014	2019-04	
14.10	Utopic Unicorn	23-10-2014	2015-07	
15.04	Vivid Vervet	23-04-2015	2016-01	

Warna	Arti
Merah	Sudah tidak didukung
Hijau	Masih didukung
Biru	Rilis masa depan

Gambar II-8 Versi Rilis Ubuntu

- **Ubuntu 4.10 (Waty Wathog)**

  Inilah cikal bakal Ubuntu, yang diluncurkan tanggal 20 Oktober 2004. Kode namanya adalah Warty Warthog dengan nomor kode 4.10 yang muncul dengan logo sedikit aneh yaitu babi hutan. Rilis ini dilanjutkan dengan komitmen untuk secara simultan melakukan update security untuk jangka waktu 18 bulan sesuai dengan rangkaian Ubuntu Security Notices pada saat itu. Tampilan desktop yang indah membuat Ubuntu 4.10 menjadi idola di rumah, sekolah dan bisnis hampir diseluruh belahan dunia. Pada sat itu

masih belum banyak Linux Desktop berbasis grafis yang memiliki tampilan interface menarik. Beberapa fitur lainnya adalah instalasi cepat dan sederhana, ketersediaan paket secara online, sudah terintegrasi baik dengan pengguna laptop, Firefox 0.9, Evolution 2.0, OpenOffice.org 1.1.2 dan juga dukungan untuk hardware. Server Ubuntu 4.10 bisa diinstalasikan dengan mode minimalis.

- **Ubuntu 5.04 (Hoary Hedgehog)**

  Kode nama Hoary Hedgehog adalah rilis Ubuntu kedua yang dikeluarkan dengan kode nomor 5.04 pada tanggal 8 April 2005. Icon yang digunakan adalah binatang landak. Pada versi ini merupakan awal mula dari Kubuntu, yaitu distro Linux Ubuntu yang berbasiskan KDE sebagai desktop environment. KDE yang digunakan pada Kubuntu ini adalah versi 3.4, sedangkan Ubuntu sendiri menggunakan basis GNOME versi 2.10. Pada versi ini terdapat fasilitas baru untuk melakukan update yang dapat berjalan pada modus background. Prooses booting pada versi ini sudah lebih cepat dibanding versi pendahulu. Pun demikian versi ini lebih banyak mengenali hardware pada komputer. Versi ini juga mendukung instalasi melalui media USB serta men-support program kompresi bzip2, autentifikasi Apt dan juga sudah adanya versi Live CD yang memungkinkan anda menggunakan Ubuntu tanpa perlu di-install terlebih dahulu.

- **Ubuntu 5.10 (Breezy Badger)**

  Rilis ketiga dari Ubuntu ini menggunakan binatang jenis luwak sebagai icon-nya. Distro yang dirilis pada 13 Oktober 2005 ini hadir dengan GNOME sebagai desktop *environment* dan didalamnya sudah terpasang program aplikasi OpenOffice versi 2.0 beta 2. Untuk memperkaya content-nya, hadir juga EDUbuntu, yaitu jenis baru dari Ubuntu yang berfokus dalam dunia pendidikan. EDUbuntu berisi aplikasi-aplikasi edukatif dan dapat digunakan oleh siswa untuk sarana belajar. Didalamnya terdapat aplikasi matematika, fisika, kimia, serta aplikasi edukatif lainnya. Fitur-fitur tambahan pun banyak ditemui pada versi ini seperti hadirnya usplash, yaitu loading bar pada saat proses Ubuntu. Fitur lainnya berupa dukungan untuk menulis audio CD, tambahan *driver hardware* dari *third party*, dukungan

penuh untuk printer dan *scanner Hewlett-Packard*, kompatibilitas keyboard dan mouse Bluetooth, serta kernel 64-bit untuk Power PC.

- **Ubuntu 6.06 (Dapper Drake)**

  Rilis keempat muncul pada tanggal 1 Juni 2006 dengan nama Dapper Drake dan berkode nomor 6.06. Icon versi ini adalah binatang bebek. Versi ini muncul dengan basis GNOME dan KDE. Keluarnya *Dapper Drake* menandai semakin bertambahnya jumlah pengguna Ubuntu di Indonesia. Bersamaan dengan momen ini bermunculan pula tempat download lokal di Indonesia. Fitur terbaru yang disertakan adalah cara instalasi melalui Live CD secara cepat, sistem start-up yang singkat pada saat login, menu yang simple, proses shutdown dengan visual grafis, dukungan terhadap video playback dan pre install dengan paket aplikasi openOffice 2.0.2. Dari versi ini lahir jenis baru yaitu Xubuntu. Perbedaannya dengan Ubuntu, Kubuntu dan EDUbuntu adalah desktop environment yang digunakan Xubuntu merupakan XFCE versi 4.3.90.1. Desktop environment ini relatif lebih ringan dibandingkan dengan GNOME atau KDE.

- **Ubuntu 6.10 (Edgy Eft)**

  Pada tanggal 26 Oktober 2006 rilis kelima Ubuntu Edgy Eft muncul. Ubuntu bermaskot kadal berwarna oranye ini memiliki peningkatan performa pada start-up dan shutdown speed serta terintegrasi dengan Tomboy dan F-Spot. Fitur dan content yang dibenamkan antara lain kernel 2.16.17, Evolution 2.8.0, Firefox 2.0 dan OpenOffice 3.0.4. Desktop environment menggunakan GNOME2.16, KDE 3.5.5 dan XFCE 4.3.99 RC1. Pada versi ini terdapat sedikit keistimewaan karena banyaknya aplikasi tambahan diantaranya beryl, xgl dan compiz. Aplikasi-aplikasi add on ini menjadikan tampilan desktop Ubuntu semakin memukau. Ubuntu 6.10 mencuri perhatian orang-orang dan digunakan sebagai pilihan alternatif bagi sistem operasi Microsoft Windows

- **Ubuntu 7.04 (Feisty Fawn)**

  Ubuntu generasi ke-6 ini dirilis pada tanggal 19 April 2007 dengan nama Feisty Fawn, yang menggunakan icon seekor kancil afrika. Didalamnya telah terdapat kernel Linux 2.6.20, desktop GNOME 2.18, KDE 3.5.6 dan

XFCE 4.4. Namun Ubuntu 7.04 ini meminta penggunaan memori RAM minimal 256 MB agar bisa dijalankan di komputer. Pada versi ini mulai digunakan edisi Alternate. Edisi ini digunakan jika anda ingin meng-install dengan waktu yang lebih singkat dibandingkan dengan menggunakan grafis. Fitur terbarunya adalah tool migrasi Windows yang memudahkan integrasi antara aplikasi Windows dan Ubuntu jika anda menggunakan dual booting. Fitur lainnya berupa kemudahan instalasi media codec, serta plug dan play jaringan menggunakan Avahi.

- **Ubuntu 7.10 (Gutsy Gibbon)**

  Pada tanggal 15 Oktober 2007 Ubuntu teranyar dengan nama Gutsy Gibbon dirilis oleh Canonical Ltd. Versi ini menggunakan hewan siamang sebagai maskot icon-nya. Keunggulan pada rilis ini antara lain adalah adanya dukungan add-on atau plugin untuk web browser firefox, wizard untuk dukungan printer, WiFi, kamera digital, IPod dan piranti digital lainnya. Versi ini juga sudah mendukung akses ke system file NTFS secara default. Di versi sebelumnya, tidak memiliki kemampuan untuk membaca system file NTFS. Efek 3D juga disetel secara default jika semua persyaratan minimumnya sudah terpenuhi. Untuk mendukung keamanan jaringan disediakan Apparmor dari Novell. Pun ditambahkan desktop search, switch user yang cepat, dan dukungan untuk thin client atau biasa disebut LTSP (Linux Terminal Server Project).

- **Ubuntu 8.04 (Hardy Heron)**

  Pada 24 April 2008, Ubuntu terbaru muncul dengan kode nama Hardy heron. Ubuntu 8.04 berlambang burung bangau ini mensyaratkan memory RAM minimal sebesar 384 MB. Bertambahnya konsumsi RAM yang semakin besar dikarenakan semakin ciamiknya tampilan grafis dan juga untuk dukungan aplikasi-aplikasi yang digunakan. Hardy Heron merupakan versi LTS (Long Term Support) yaitu paket yang dimiliki oleh Ubuntu 8.04 yang akan didukung selama jangka waktu 3 tahun untuk varian desktop dan 5 tahun untuk varian server. Dukungan ini juga dapat anda temui pada Ubuntu Dapper Drake. Pada versi ini juga muncul istilah Wubi, yaitu installer Ubuntu di dalam OS Windows. Anda tidak perlu memasang

Ubuntu ke dalam harddisk komputer. NFS (*Network File System*) juga sudah didukung di dalam versi ini.

- **Ubuntu 8.10 (Intrepid Ibex)**

  Ubuntu 8.10 Intrepid Ibex dirilis pada tanggal 30 Oktober 2008. Ubuntu ini dapat dijalankan dengan minimal RAM sebesar 256 MB asalkan kapasitas RAM tidak di-share dengan kartu grafis. Ubuntu 8.10 dirancang untuk gaya hidup digital karena banyak fitur-fitur yang mendukung untuk hal ini. Fitur yang dimiliki Ubuntu 8.10 antara lain adalah dukungan jaringan 3G dengan menggunakan kabel ataupun WiFi. Pada rilis ini juga banyak modem-modem dan juga handphone untuk ber-internet ria sudah dikenali dan anda tidak perlu melakukan pengaturan yang rumit. Intrepid Ibex juga mendukung instalasi melalui live USB.

- **Ubuntu 9.04 (Jaunty Jackalope)**

  Jaunty Jackalope dirilis tanggal 23 April 2009 dengan menggunakan maskot icon kelinci bertanduk. RAM minimum yang diperlukan untuk menjalankan versi ini sebesar 256 MB, namun disarankan menggunakan ukuran yang lebih besar. Keunggulan Ubuntu 9.04 ini salah satunya adalah speed booting hanya sekitar kurang lebih 25 detik. Dukungan 3G dan wireless juga disertakan dari versi sebelumnya. Paket OpenOffice yang digunakan adalah versi 3.0. Aplikasi-aplikasi seperti Ubuntu Tweak yang memudahkan anda mengatur sistem hingga manajemen paket dari third party sudah tersedia untuk ubuntu ini. Desktop yang digunakan adalah GNOME 2.26. Perbedaan utama rilis ini dengan versi lain adalah system file Ext4 yang merupakan file sistem terbaru dari Linux setelah Ext3. File sistem ini lebih tahan uji dan stabil karena merupakan penyempurnaan dari system file Ext3.

- **Ubuntu 9.10 (Karmic Koala)**

  Karmic Koala merupakan rilis kandidat yang sesuai jadwal keluar pada tanggal 29 Oktober 2009, dengan lambang Koala. Ubuntu rilis kali ini menyertakan GNOME 2.28.1, KDE 4.3.1, OpenOffice 3.1.1 dan kernel Linux 2.6.31. Karmic Koala mengganti arsitektur akselerasi grafis X.Org server EXA menjadi UXA karena adanya masalah pada driver video Intel tersebut. Pada versi ini, aplikasi-aplikasi yang disertakan semakin lengkap

diservarian baru maupun penambahan fitur dan performa. Karmic Koala sudah mampu mengakomodasi semua kebutuhan komputerisasi user secara total.

- **Ubuntu 10.4 (Lucid Lynx)**

  Pada tanggal 27 April 2010, Canonical Ltd mengumumkan rilis Ubuntu 10.4 Lucid Lynx. Kelebihan versi Ubuntu bermaskot kucing gunung ini antara lain boot speed akan terasa lebih cepat pada hampir semua komputer, dan terasa sangat cepat pada komputer berbasis SSD seperti netbook. Aplikasi ubuntu One yang disertakan pada versi ini berguna pada peningkatan integrasi desktop untuk online services serta sharing file dan folder via internet dengan lebih cepat dan mudah. Kernel Linux yang digunakan Lucid Lynx adalah versi 2.6.32-16.25 based on 2.6.32.9. Desktop environment menggunakan GNOME dan KDE. Selain itu dibenamkan pula HAL Removal yang membuat akselerasi dan boot Ubuntu semakin cepat. Indikator-indikator baru pada desktop juga banyak bermunculan pada versi ini.

- **Ubuntu 10.10 (Maverick Meerkat)**

  Canonical Ltd merilis versi ini pada tanggal 10 Oktober 2010. Ubuntu 10.10 memiliki dukungan multi-touch. Hal ini dimungkinkan melalui uTouch Ubuntu 1.0 dan multi-touch stack. Dengan Ubuntu 10.10, berbagai aplikasi GTK mendapat dukungan gesture-based scrolling. Selain itu, document viewer Ubuntu pun disempurnakan Canonical agar mendukung interaksi yang lebih baik. Untuk teknologi multi-touch baru, Canonical bekerja sama dengan X.Org dan komunitas kernel Linux, untuk menambahkan dukungan fitur yang belum ada atau memperbaiki driver yang telah ada. Tampilan graphical Maverick Meerkat sangat menawan, akselerasi ke menu-menunya sangat mudah dan cepat diseranimasi yang memukau. Diperkirakan versi ini akan menjadi batu lompatan generasi Linux Ubuntu selanjutnya menggunakan graphical sentuh serta dukungan penuh untuk multimedia mobile.