BAB 2
TINJAUAN PUSTAKA

2.1 Profil Perusahaan

Berikut ini adalah tinjauan umum profil singkat perusahaan PT. Duta Transformasi Insani sebagai tempat penelitian, yaitu :

2.1.1 Sejarah Singkat Perusahaan

Pendirian perusahaan ini adalah diawali dari ditetapkannya rencana strategis Daarut Tauhid 2022 yang mendorong terjadinya sinergi aktivitas yang ada di lingkungan pesantren Daarut Tauhid, salah satu lini yang paling strategis adalah bidang pelatihan. Sebelumnya terdapat dua lembaga pelatihan dalam lingkungan Daarut Tauhid, yaitu Daarut Tauhid *Training Center* (DTTC) yang merupakan unit kerja di Yayasan Daarut Tauhid dan LP2ES *Learning Center* yang merupakan unit usaha Kopontren Daarut Tauhid.

Sebagai upaya untuk mensinergikan dan mengembangkan peran dan kiprah Daarut Tauhid di bidang pelatihan sumber daya manusia, maka pada tanggal 1 Mei 2013 didirikanlah perusahaan berbentuk PT (Perseroan Terbatas) yang merupakan hasil *merger* dari dua unit pelatihan tersebut dan diberi nama PT. Duta Transformasi Insani (PT. DT Insani) dengan Yayasan Daarut Tauhid, Kopontren Daarut Tauhid, dan KH Abdullah Gymnastiar sebagai pemegang sahamnya. Bidang usaha dari perusahaan ini adalah (1) Pendidikan dan Pelatihan, (2) Konsultan Manajemen, (3) *Event Organizer*, dan (4) Laboratorium Bisnis.

2.1.2 Logo Instansi

Gambar 2.1 berikut adalah logo resmi perusahaan yang digunakan oleh PT. Duta Transformasi Insani :



Gambar 2.1 Logo PT. Duta Transformasi Insani

Bentuk keseluruhan logo ini merupakan penggabungan huruf ‘d’, ‘t’, ‘i’ dalam satu karakter. Unsur pita dan berlian melambangkan proses perjalanan (pita) menuju suatu tujuan (berlian). Perjalanan dalam rangka perubahan ini merupakan proses yang berkelanjutan, karena itu tujuan yang dicapai merupakan awal dari proses perjalan berikutnya, yang digambarkan oleh pita yang keluar lagi dari berlian. Ini menggambarkan suatu proses perjalanan yang terus-menerus untuk selalu menjadi lebih baik dan lebih baik lagi.

2.1.3 Visi dan Misi

Perusahaan PT.Duta Transformasi Insani memiliki visi dan misi, yaitu:

1. Visi

   Menjadi konsultan manajemen yang terbaik dan terpercaya di Indonesia dalam pengembangan karakter baik dan kuat pada tahun 2020.

2. Misi
   a. Membangun bangsa yang berkarakter baik dan kuat menuju kebahagian dunia dan akhirat.
   b. Memberikan konsultansi manajemen dengan pelayanan terbaik, memuaskan, kreatif inovatif dan berkesinambungan.
   c. Membangun lembaga berkah, sehat, kuat terpercaya, serta berdaya saing yang dikelola oleh sumber daya manusia ahli dzikir, fikir dan ikhtiar.

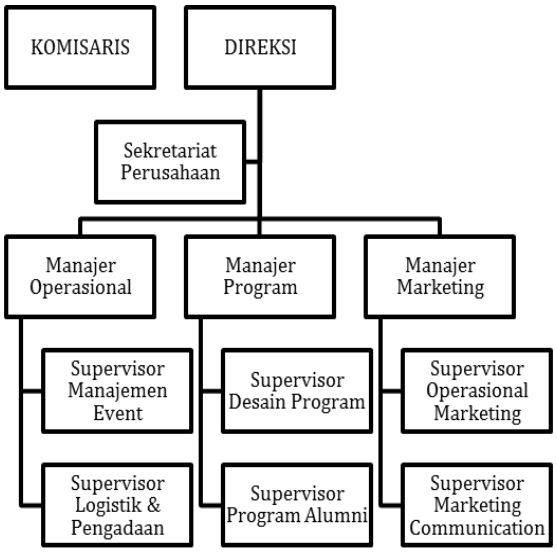
3. Tujuan

   Memberikan manfaat dan solusi dalam pengembangan sumber daya manusia.

2.1.4 Struktur Organisasi

Organisasi adalah tempat atau wadah orang berkumpul untuk saling bekerjasama untuk mencapai tujuan dan manfaat bersama. Dengan demikian dapat dikatakan bahwa struktur organisasi pada suatu organisasi merupakan kerangka dasar yang menggambarkan alur hubungan antara bagian yang satu dengan yang lainnya,

sehingga suatu bagian dalam organisasi tersebut menjadi jelas kedudukan, jabatan, wewenang, dan tanggung jawabnya.



Gambar 2.2 Struktur Organisasi PT. Duta Transformasi Insani

2.1.4.1 Deskripsi Kerja

Pada perushaan ini memiliki beberapa bidang kerja dan pegawai. Adapaun disebut pegawai ialah mulai dari *level* kepala sekretariat, *manager*, *supervisor*, dan *staff*, sedangkan direksi dan komisaris tidak termasuk dalam kategori pegawai. Dan berikut ini penjelasan mengenai fungsi pokok dari masing-masing bidang yang dideskripsikan sebagai berikut:

1. **Komisaris**

Melakukan pengawasan terhadap kebijakan pengurusan perusahaan yang dilakukan direksi serta memberi nasihat kepada direksi termasuk mengenai rencana pengembangan perusahaan, rencana jangka panjang, rencana kerja dan anggaran perusahaan, pelaksanaan ketentuan-ketentuan anggaran dasar dan keputusan RUPS (Rapat Umum Pemegang Saham) dan peraturan perundang-undangan yang berlaku.

2. **Direksi**

Direksi merupakan organisasi perusahaan yang bertanggung jawab penuh atas pengurusan perusahaan untuk kepentingan dan tujuan Perusahaan serta mewakili perusahaan baik di dalam maupun di luar pengadilan sesuai ketentuan anggaran dasar.

3. Sekretariat

Merencanakan, mengembangkan, dan mengontrol fungsi administrasi, keuangan, dan personalia di perusahaan sehingga dapat memberikan informasi keuangan secara komprehensif dan tepat waktu untuk membantu perusahaan dalam proses pengambilan keputusan yang mendukung pencapaian target keuangan perusahaan.

4. Operasional

Merencanakan, mengarahkan dan mengendalikan semua sumber daya untuk menyelenggarakan operasional *event*/pelatihan dengan efektif, efisien, memenuhi standar kualitas program/layanan yang persyaratkan, dan memberikan sigma kepuasan kepada *customer*.

5. Marketing

Merencanakan, mengarahkan dan mengendalikan seluruh kegiatan pemasaran program/layanan perusahaan serta mengembangkan hubungan dengan *customer*.

6. Program

Merencanakan, mengarahkan dan mengendalikan seluruh kegiatan pengembangan program atau layanan yang sesuai dengan kebutuhan *customer* dan mendukung pencapaian visi, misi, dan tujuan perusahaan.

2.2 Landasan Teori

Berikut ini adalah beberapa landasan teori yang digunakan oleh penulis sebagai pendukung teori dasar dari perancangan dan implementasi jaringan *small office home office* berbasis *network attached storage* di PT. Duta Transformasi Insani.

2.2.1 Jaringan Komputer

Jaringan komputer adalah sekelompok komputer otonom yang saling berhubungan antara satu dengan lainnya menggunakan protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, program-program, penggunaan bersama perangkat keras seperti *printer*, *hard disk*, dan sebagainya.

Selain itu jaringan komputer bisa diartikan sebagai kumpulan terminal komunikasi yang berada di berbagai lokasi yang terdiri dari lebih satu komputer yang saling terhubung [2].

2.2.1.1 Manfaat Jaringan Komputer

Adapun manfaat yang didapat dalam membangun jaringan komputer adalah sebagai berikut [2] :

a. *Sharing resources,* bertujuan agar seluruh program, peralatan atau *peripheral* lainnya dapat dimanfaatkan oleh setiap orang yang ada pada jaringan komputer tanpa terpengaruh oleh lokasi maupun pengaruh dan pemakai.

b. Media komunikasi, jaringan komputer memungkinkan terjadinya komputer antar pengguna, baik untuk *teleconference* maupun untuk mengirim pesan atau informasi yang penting lainnya. Dengan menggunakan jaringan komputer, dua orang atau lebih yang jaraknya sangat jauh akan lebih mudah bekerja.

c. Integrasi data, pembangunan jaringan komputer dapat mencegah ketergantungan pada komputer pusat, setiap proses data tidak harus dilakukan pada satu komputer saja, melainkan dapat didistribusikan ke tempat lainnya.

d. Pengembangan dan pemeliharaan, dengan adanya jaringan komputer ini, maka pengembangan peralatan dapat dilakukan dengan mudah dan menghemat biaya. Jaringan komputer juga bisa memudahkan pemakai dalam merawat *hard disk* dan peralatan lainnya, seperti memberikan perlindungan terhadap serangan *virus* maka pemakai cukup memusatkan perhatian pada *hard disk* uang ada di komputer pusat.

e. Keamanan data, memberikan perlindungan terhadap data. Jaminan keamanan data tersebut diberikan melalui pengaturan hak akses para pemakai dan *password*, serta teknik perlindungan terhadap *hard disk* sehingga data mendapatkan perlindungan yang efektif.

Agar dapat mencapai tujuan yang sama, setiap bagian jaringan komputer meminta dan memberikan layanan. Pihak meminta layanan disebut *client* dan pemberi layanan disebut *server.* Arsitektur ini disebut dengan sistem *client-server* yang digunakan pada hampir seluruh jaringan komputer.

2.2.1.2 Klasifikasi Jaringan Komputer

Pengklasifikasian jaringan komputer secara garis besar terdiri dari klasifikasi utama, yaitu [2] :

1. Berdasarkan Topologi
2. Berdasarkan Geografis
3. Berdasarkan Fungsi

Pada kenyataanya, klasifikasi jaringan komputer masih terus berkembang dengan berkembangnya jaringan komputer dunia. Penjelasan dari masing-masing klasfikasi tersebut di atas adalah sebagai berikut :

1. Berdasarkan Topologi

Topologi jaringan adalah bagaimana jaringan itu tersambung secara fisik atau logika. Model topologi yang umum dibangun saat ini ada tiga model dasar, yaitu *star*, *bus*, dan *ring*. Selain ketiga model tersebut masih terdapat model lainnya, hanya saja merupakan penggabungan dari tiga model topologi tadi.

2. Berdasarkan Geografis

Cakupan geografis jaringan komputer secara umum dibagi atas tiga jenis, yaitu :

a. Local Area Network

LAN (*Local Area Network)* merupakan satuan terkecil dari jenis cakupan jaringan komputer, contohnya jenis jaringan LAN adalah jaringan internal kampus/sekolah, kantor, warung internet.

b. Metropolitan Area Network

MAN (*Metropolitan Area Network)* merupakan satuan menengah dari jenis cakupan jaringan komputer, contoh jaringan MAN adalah jaringan publik diimplementasikan di dalam satu kota.

c. Wide Area Network

WAN (*Wide Area Network)* merupakan cakupan terluas dari jenis cakupan jaringan komputer lainnya. Jaringan ini disamakan dengan jaringan internet, karena lingkungannya yang begitu luas, hingga jaringan antar kota, negara, bahkan benua.

3. Berdasarkan Fungsi

Dalam dunia jaringan, dikenal dua buah fungsi komputer yang terhubung ke suatu jaringan sebagai *client, server,* atau memiliki kedua fungsi tersebut sekaligus.

Sifat utama dari komputer yang memiliki *level client* biasanya aktif meminta data ke *server,* memiliki antarmuka grafis, dan berada pada daerah yang mudah diakses manusia. Sedangkan *server* bersifat pasif, hanya menunggu sampai ada permintaan dari *client* baru beraktifitas, tidak disertai antarmuka *grafis,* dan biasanya terletak di suatu tempat yang tersembunyi dan tidak mudah diakses oleh sembarang orang. Klasifikasi jaringan secara umum dibagi atas dua jenis secara fungsi, yaitu :

a. Peer to peer

Fungsi *peer to peer* pada suatu jaringan komputer terjadi saat semua komputer yang saling terhubung memiliki fungsi setara, yaitu sebagai *client* sekaligus *server.*

b. Client-Server

Fungsi *client-server* pada suatu jaringan komputer terjadi apabila ada satu atau lebih komputer yang berfungsi sebagai *client* saja dan ada satu atau lebih komputer yang berfungsi sebagai *server* saja dan keduanya saling terhubung dalam jaringan komputer.

2.2.1.3 Elemen Keamanan

Keamanan merupakan kondisi dimana informasi dan infrastruktur berada dalam keadaan baik, tidak terdeteksi adanya pencurian data dan tidak ada gangguan terhadap layanan informasi atau berada pada tingkat yang dapat ditoleransi. Elemen terkait dalam penerapan keamanan, adalah [3] :

a. Kerahasiaan

Mampu menjaga kerahasiaan isi dan sumber informasi dari pihak yang tidak berhak.

b. Keasliaan

Informasi yang diberikan merupakan informasi yang terjamin keasliannya dan tidak mengalami perubahan dari sumber informasi.

c. Integritas

Data dan informasi terjaga akurasi dan kelengkapannya.

d. Ketersediaan

Menjamin bahwa informasi dapat diakses dan digunakan oleh pihak yang berwenang ketika dibutuhkan. *Avaibality* dipengaruhi oleh 3 faktor, yaitu :

a. Frekwensi dari *downtime*
b. Durasi dari *downtime*
c. Dampak

2.2.1.4 Tipe Serangan

Serangan dapat didefinisikan sebagai penyerangan terhadap keamanan sistem oleh ancaman berkecerdasan atau aksi dengan metode dan teknik tertentu guna mengecoh sistem keamanan dan melanggar kebijakan keamanan sistem. Serangan yang terjadi secara garis besar dapat dikategorikan menjadi dua [3]:

1. Active Attacks

Serangan jenis ini merupakan serangan dengan metode penyerangan secara langsung pada target komputer, pada umumnya berupa serangan terhadap ketersediaan dan layanan komputer *server* sehingga berdampak pada integritas dan keaslian informasi pada sistem.

2. Passive Attacks

Serangan jenis ini dilancarkan dengan tanpa mengganggu kondisi sistem. Metode yang dilakukan adalah dengan memantau lalu lintas paket data yang ada kemudian dilakukan analisis berdasarkan frekwensi lalu lintas paket data tersebut.

Ditinjau dari sisi organisasi, serangan dapat juga dikategorikan menjadi dua, yaitu serangan pihak internal dan eksternal.

1. Serangan dari eksternal adalah serangan yang berasal dari luar organisasi pihak yang tidak memiliki hak akses mencoba melanggar kebijakan keamanan.
2. Serangan dari internal merupakan serangan yang dilancarkan oleh pihak dalam organisasi yaitu orang yang memiliki wewenang atau hak akses namun disalahgunakan atau seseorang yang mencoba menaikan tingkat hak aksesnya.

2.2.1.5 Metode Pengamanan

Metode pengamanan yang dapat dilakukan untuk mengamankan sebuah sistem sangat beragam, setiap organisasi memiliki cara dan metode masing-masing, namun secara garis besar, metode pengamanan yang dilakukan dapat dikategorikan sebagai berikut :

a. Authentikasi

Metode autentikasi paling umum digunakan adalah penggunaan *username* dan *password. User* dengan *username* dan *password* yang tepat akan terautentikasi dan dapat mengakses layanan. Jenis penggunaan metode ini ada bermacam, berikut adalah ragam metode tersebut :

1. Tidak ada *username/password*
2. Statis *username / password*
3. *Expired username / password*
4. *One-Time Password* (OTP)

b. Enkripsi

Enkripsi merupakan proses merubah informasi dari bentuk yang dapat dimengerti menjadi bentuk yang tidak dapat dimengerti. Penerima informasi yang telah dienkripsi harus melakukan proses dekripsi atau membalikan proses enkripsi agar pesan yang diterima dapat dimengerti.

Pesan yang akan dienkripsi dikenal dengan *plaintext* yang ditransformasikan berdasarkan sebuah kunci (*key)*. Hasil dari proses enkripsi dikenal dengan *chipertext* yang kemudian ditransmisikan dari *sender* menuju *receiver.*

c. Firewall

Fungsi utama dari *firewall* adalah untuk memusatkan akses *control* antara jaringan terpercaya dan tidak terpercaya. *Firewall* memiliki fungsi keamanan sebagai berikut [4] :

1. Melakukan pemblokiran terhadap lalu lintas jaringan yang tidak diinginkan.
2. Mengarahkan lalulintas yang masuk pada sistem internal yang lebih dapat dipercaya.
3. Menyembunyikan sistem yang rentan, yang tidak mudah diamankan dari internet.
4. Membuat log lalu lintas dari dan menuju jaringan pribadi.
5. Dapat memberikan sistem autentikasi yang kuat.

d. Vulnerability Patching

Melakukan penutupan lubang keamnan yang ditemukan guna mengurangi risiko kehilangan atau kerusakan sistem. Metode yang dilakukan diantarnya :

1. *Software Update*

   Sistem operasi atau program aplikasi yang memiliki celah kemanan dapat diperbaharui sehingga program aplikasi tersebut bebasdari celah kemanan yang telah diketahui.

2. *Software Security*

   Melakukan instalasi perangkat lunak penunjang kemanan guna meningkatkan keamanan, dapat berupa oerangkat keamanan *host based* maupun *network based* untuk mencegah atau memantau sistem yang bekerja.

2.2.2 Small Office Home Office

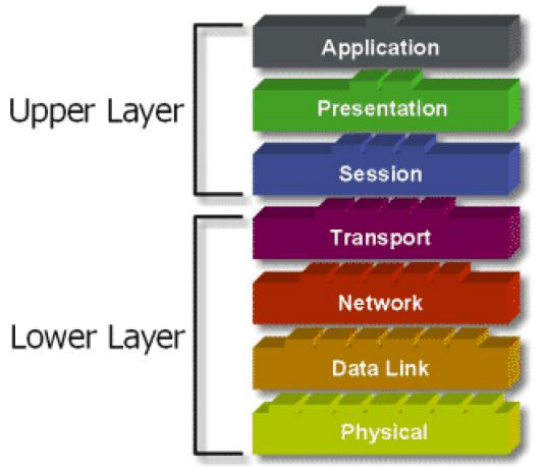
Small Office Home Office (SOHO) adalah istilah yang mengacu pada bisnis atau usaha kecil yang dilakukan di rumah. Mobilitas yang semakin tinggi dan semakin terbatasnya jarak dan waktu membuat rumah bisa sebagai pilihan untuk melakukan usaha dengan nilai strategis yang tinggi.

2.2.3 Open Systems Interconnection

Model *Open Systems Interconnection* (OSI) diciptakan oleh *International Organization for Standardization* (ISO) yang menyediakan kerangka logika terstruktur bagaimana proses komunikasi data berinteraksi melalui jaringan. Standar ini dikembangkan untuk industri komputer agar komputer dapat berkomunikasi pada jaringan yang berbeda secara efisien [5].

Tujuan utama penggunaan model OSI adalah untuk membantu desainer jaringan memahami fungsi dari tiap-tiap *layer* yang berhubungan dengan aliran komunikasi data. Termasuk jenis jenis protokol jaringan dan metode transmisi.

Model dibagi menjadi 7 *layer*, dengan karakteristik dan fungsinya masing-masing. Setiap *layer* harus dapat berkomunikasi dengan *layer* di atasnya maupun di bawahnya secara langsung melalui serentetan protokol.



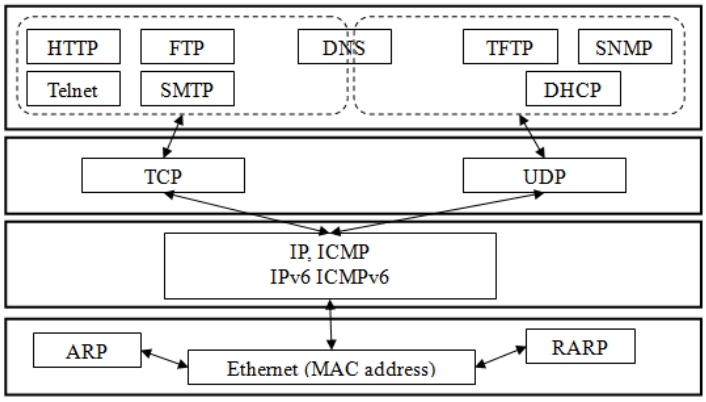
Gambar 2.3 Model 7 OSI Layer

(Sumber: http://vengenzblog.blogspot.com/2013/03/7-layer-osi.html)

Berikut adalah definisi dari masing-masing OSI *layer*, yaitu :

1. *Layer Application*

Layer paling tinggi dari model OSI, seluruh layer di bawahnya bekerja untuk layer ini, tugas dari *application layer* adalah berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. Gambar 2.4 berikut ini adalah beberapa protokol yang bekerja pada *application layer* :



Gambar 2.4 Application Layer Protocols

(*Sumber: http://wiki.mikrotik.com/wiki/Testwiki/Introduction_to_internetworking)*

Protokol yang terdapat pada *application layer* memiliki tentang *header information* dan prinsip kerja *protocol* yang berbeda-beda, yaitu :

a. Hypertext Transfer Protocol

HTTP (*Hypertext Transfer Protocol*) adalah sebuah protokol jaringan lapisan aplikasi yang digunakan untuk sistem informasi terdistribusi, kolaboratif, dan menggunakan hipermedia. Gambar 2.5 berikut ini adalah *header information* yang terdapat pada HTTP :

Request Line	General Header	Request Header	Entity Header	Message Body

Gambar 2.5 HTTP Header Information

(Sumber: http://wiki.mikrotik.com/wiki/Testwiki/Introduction_to_internetworking)

b. File Transfer Protocol

FTP (*File Transfer Protocol*) adalah protokol yang berfungsi untuk tukar-menukar *file* dalam suatu jaringan yang menggunakan TCP untuk proses koneksi.

FTP *server* adalah suatu *server* yang menjalankan perangkat lunak yang berfungsi untuk memberikan layanan tukar menukar *file*, dimana *server* tersebut selalu siap memberikan layanan FTP apabila mendapat permintaan dari FTP *client.*

Tujuan dari FTP *server* adalah sebagai berikut :

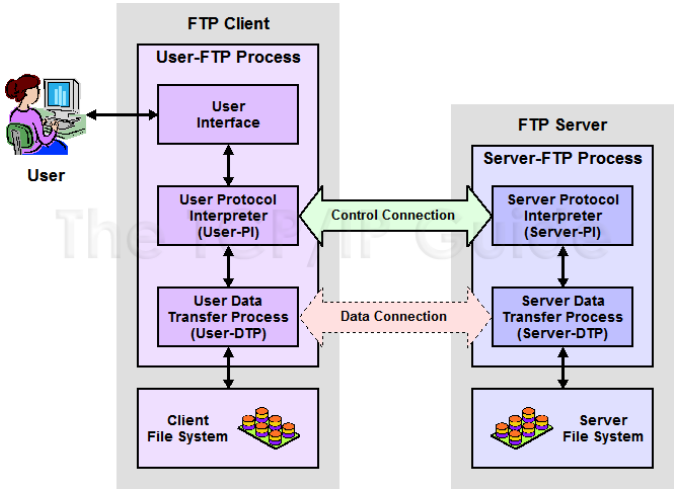
a. *Sharing data*

b. Menyediakan *indirect* atau *implicit remote* komputer

c. Menyediakan tempat penyimpanan bagi pengguna

d. Menyediakan transfer data yang *reliable* dan efisien

FTP *client* adalah komputer yang meminta koneksi ke FTP *server* untuk tujuan tukar menukar *file*. Setelah terhubung dengan FTP *server*, maka *client* dapat melakukan *download, upload, rename, delete,* dll sesuai dengan hak akses yang diberikan oleh *administrator*. Gambar 2.6 berikut ini adalah prinsip kerja yang terdapat pada *file transfer protocol*:



Gambar 2.6 Prinsip Kerja FTP

(Sumber : http://yantosimamora.blogspot.com/2012/05/konsep-komponen-dan-fungsi-ftp-server.html)

c. Common Internet File System

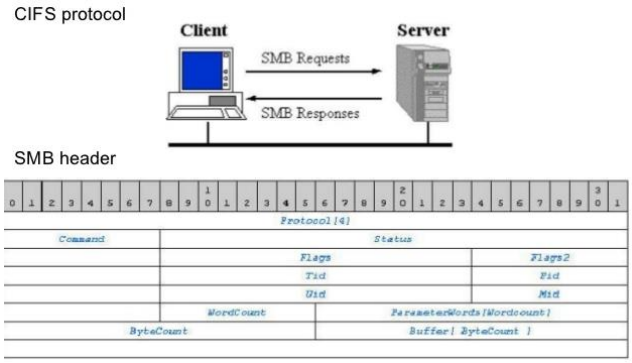
CIFS (*Common Internet File System*) merupakan sebuah implementasi dari protokol *file-sharing* SMB (*Server Message Block*) yang telah diusulkan agar menjadi standar internet, sehingga dapat diperoleh secara mudah. Perbedaan dari protokol SMB adalah bahwa protokol ini telah diperbaiki agar dapat digunakan melalui Internet. Protokol ini merupakan "saingan tidak langsung" dari protokol NFS (*Network File System)* yang digunakan dalam keluarga sistem operasi Unix. Protokol ini menggunakan arsitektur c*lient-server*.

CIFS telah dilihat sebagai kemungkinan pengganti protokol *File Transfer Protocol* (FTP) dan *Network File System* (NFS) sebagai protokol berbagi berkas dan sistem manajemen berkas pada *platform* Windows. CIFS mendukung penggunaan

password yang terenkripsi, serta nama berkas dengan pengkodean *unicode*. Selain itu CIFS juga dapat digunakan untuk mengaitkan (*mount*) sebuah sistem berkas jarak jauh sebagai sebuah direktori atau *drive* dalam mesin lokal, seolah-olah sistem berkas jarak jauh tersebut merupakan sistem berkas lokal.

Keunggulan CIFS dibandingkan dengan protokol FTP dan HTTP sebagai protokol berbagi berkas adalah bahwa CIFS mendukung akses baca dan tulis terhadap sebuah berkas secara simultan, sementara HTTP dan FTP hanya mendukung *transfer* berkas sederhana saja.

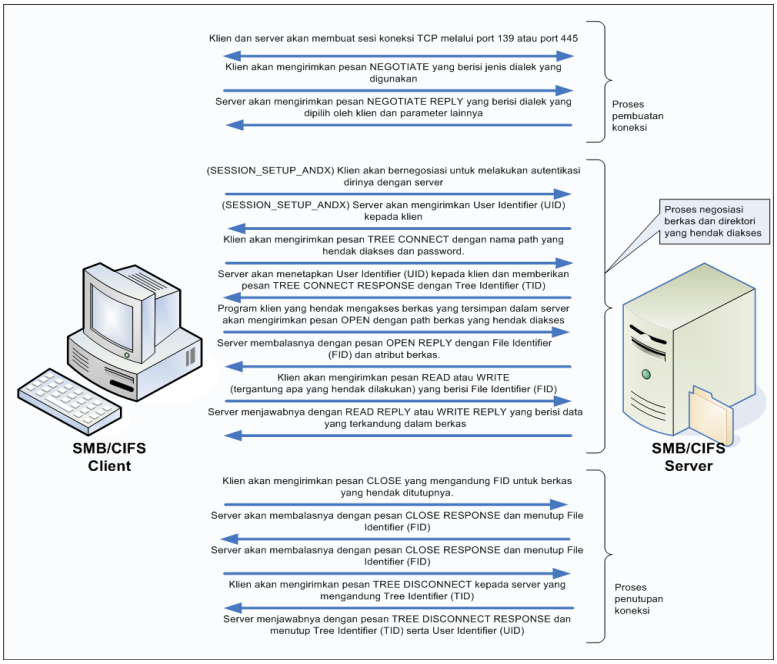
Sementara, jika dibandingkan dengan protokol NFS, CIFS menawarkan beberapa keunggulan peningkatan performa dengan adanya fitur *read-ahead, write-behind* dan *fitur opportunistic locks*. Gambar 2.7 berikut ini adalah *information header* yang terdapat pada CIFS *(Common Internet File System)* :



Gambar 2.7 SMB/CIFS Header Information

(Sumber : http://flylib.com/books/1/202/1/html/2/files/181fig01.gif)

Gambar 2.8 berikut adalah prinsip kerja yang terjadi ketika protokol CIFS/SMB2 digunakan :

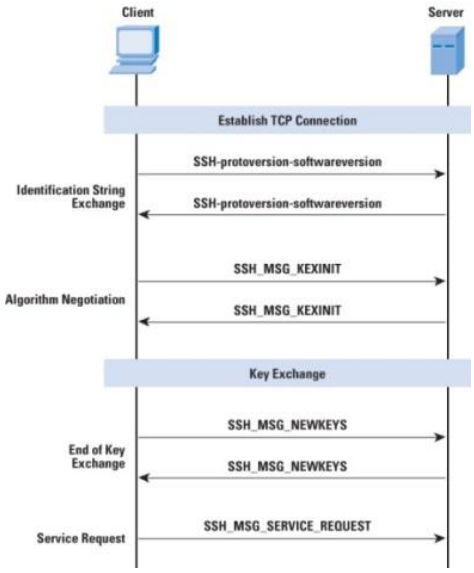


Gambar 2.8 Prinsip Kerja Protokol CIFS/SMB

(Sumber : http://upload.wikimedia.org/wikipedia/id/thumb/3/39/Negosiasi_Koneksi_CIFS.png/663px-Negosiasi_Koneksi_CIFS.png)

d. Secured Shell Protocol

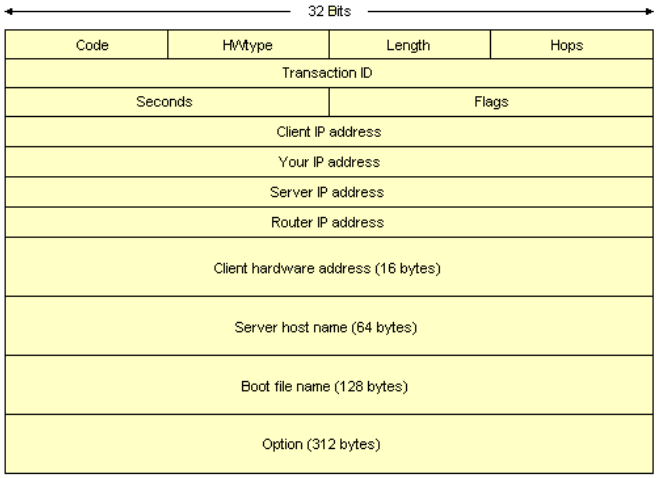
SSH (*Secure Shell Protocol*) adalah protokol jaringan yang memungkinkan pertukaran data secara aman antara dua komputer. SSH dapat digunakan untuk mengendalikan komputer dari jarak jauh mengirim *file*, membuat *tunnel* yang terenkripsi dan lain-lain. Protokol ini mempunyai kelebihan dibanding protokol sejenis seperti Telnet, FTP, Danrsh, karena SSH memiliki sistem otentikasi, otorisasi, dan enkripsi. Gambar 2.9 berikut ini adalah prinsip kerja yang terdapat pada *secure shell protocol* :



Gambar 2.9 Prinsip Kerja Protokol SSH

(*Sumber : https://nsafaat.files.wordpress.com/2011/11/ssh-tunneling.png*)

Gambar 2.10 berikut ini adalah *information header* yang terdapat pada *dynamic host configuration protocol* :



Gambar 2.10 DHCP Header Information

(Sumber:http://www.technologyuk.net/the_internet/internet/images/dhcp_frame_format.gif)

e. Simple Network Muligrapher Protocol

SNMP (*Simple Network Multigrapher Protocol*) menyediakan format komunikasi antara *agent* dan *manager*, yang nantinya untuk memantau atau mengelelola perangkat jaringan seperti PC, *switch, router , printer* dan perangkat jaringan lainnya.

SNMP *manager* adalah aplikasi *network management* yang berjalan pada PC, dan *agent* adalah *software* yang berjalan pada *device* yang akan dikelola. SNMP a*gent* bekerja untuk mengambil variabel yang berada pada *database* variabel atau yang sering disebut MIB (*Management Information Base*) dan membuatkan parameter untuk *device* tersebut.

Pengambilan informasi dari SNMP *agent* disebut GET *message* dan *message* yang menulis variabel disebut SET *message.* SNMP *manger* dipasang di *server* NMS (*Network Magement Service),* NMS akan menampilkan *value* SNMP secara periodik melalui grafik, dalam bentuk grafik *administrator* akan lebih mudah untuk melihat CPU *utilization, disk usage,* dll.

Selain SNMP GET *message,* untuk pengambilan *value* SNMP lewat MIB ada juga SNMP TRAP yaitu *message* apabila terdapat perangkat yang mengalami masalah.

2. *Layer Presentation*

Layer ini berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protokol yang berada dalam *layer* ini adalah perangkat lunak redirektor, seperti layanan *Workstation* (dalam Windows NT*)* dan juga *Network shell* (semacam Virtual Network Computing (VNC) atau RDP, ASCII, MPEG, MIDI, ASCII7, EBCDIC.

3. *Layer Session*

Layer ini berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat (*establishing),* dipelihara (*maintaining),* dan dihancurkan (*terminating).* Selain itu, di *level* ini juga dilakukan resolusi nama. Protokol yang berada dalam *layer* ini adalah SQL, X Window, DNS, NetBIOS, ASP, SCP, dan RPC.

4. *Layer Transport*

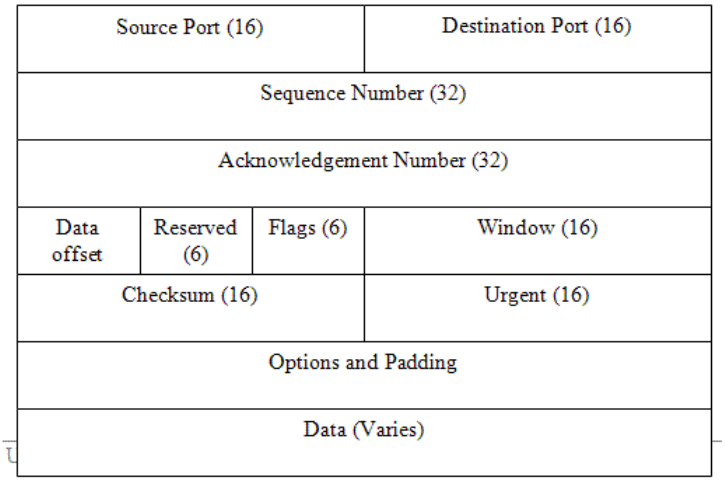
Layer ini berfungsi untuk menyediakan *end-to-end communication protocol*. *Layer* ini bertanggung jawab terhadap keselamatan data dan segmentasi data, seperti : mengatur *flow control, error detection, correcion, data sequencing,* dan *size of the packet.* Protokol yang berada dalam *layer* ini TCP, UDP, SPX, UDP, SCTP, dan IPX.

Proses pengiriman pada *transport layer* ini dapat dilakukan dengan dua mekanisme, yaitu :

a. Connection Oriented

Proses pengiriman yang menggunakan mekanisme *connection oriented* dapat diilustrasikan seperti proses pemberian pesan kepada seseorang yang dipisahkan oleh jarak yang jauh. Pemberian pesan tersebut dilakukan melalui telepon. Proses pemberian pesan akan dilakukan jika lawan bicara adalah orang yang dituju sehingga dapat dipastikan bahwa pesan yang dimaksudkan.

Dari ilustrasi tersebut dapat kita simpulkan bahwa data yang dikirimkan dengan mekanisme *connection oriented* dapat diandalkan. TCP (*Transmission Control Protocol)* merupakan jenis protokol yang mampu mengirimkan data yang *reliable* [5]. Gambar 2.11 berikut ini adalah *information header* yang terdapat pada TCP (*Transmission Control Protocol*) :

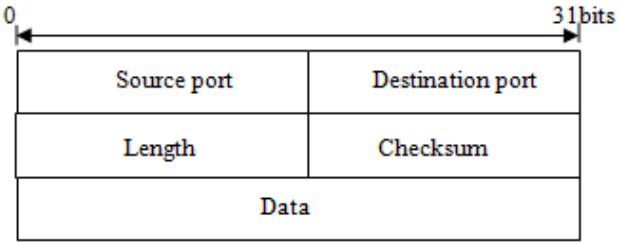


Gambar 2.11 TCP Header Information

(*Sumber : http://wiki.mikrotik.com/wiki/Testwiki/Introduction_to_internetworking*)

b. Connection Less

Mekanisme *connection less* diilustrasikan dengan proses pemberian pesan yang dilakukan melalui surat. Pengiriman surat memingkinkan sampai ke tempat tujuan belum tentu sampai ke orang yang dimaksud. Dari ilustrasi tersebut dapat disimpulkan bahwa data yang dikirimkan dengan menggunakan mekanisme *connection-less* kurang dapat diandalkan. UDP (*Unit Datagram Protocol)* mengirimkan data *unreliable* [5]. Berikut ini adalah *information header* yang terdapat pada UDP (*Unit Datagram Protocol)* :

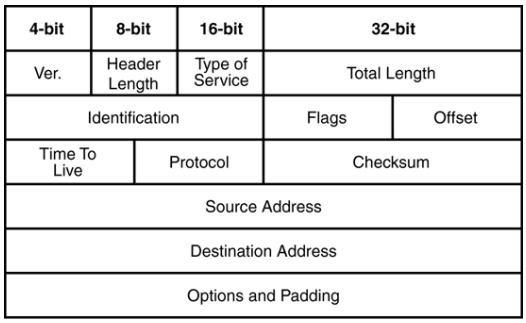


Gambar 2.12 UDP Header Information

(*Sumber : http://wiki.mikrotik.com/wiki/Testwiki/Introduction_to_internetworking*)

5. *Layer Network*

Layer ini berfungsi untuk menyediakan *logical addressing* yaitu berupa pengalamatan IP *address*, membuat *header* untuk paket-paket, dan dan *path determination*. Protokol yang berada dalam *layer* ini adalah IPX, IP, ICMP, IPSec, ARP, RIP, IGRP, BGP, OSPF, NBF, dan Q.931. Peralatan jaringan yang bekerja pada *layer* ini adalah *router*. Gambar 2.13 berikut ini adalah *information header* yang terdapat pada *IP address* (*Internet Protocol Address*) :



Gambar 2.13 IP Header Information

(*Sumber : http://wiki.mikrotik.com/wiki/Testwiki/Introduction_to_internetworking*)

6. *Layer Data Link*

Layer ini befungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut sebagai *frame*. Selain itu, pada level ini terjadi koreksi kesalahan, *flow control*, pengalamatan perangkat keras (*hardware addressing)* seperti halnya MAC *address (Media Access Control),* dan menetukan bagaimana perangkat-perangkat jaringan seperti *bridge, switch*. Spesifikasi IEEE 802, membagi *level* ini menjadi dua *level* anak, yaitu lapisan LLC (*Logical Link Control)* sebagai pengatur komunikasi seperti *error notification* dan lapisan MAC (*Media Access Control*) sebagai pengalamatan fisik yang digunakan komunikasi antar-adapter.

Protokol yang berada dalam *layer* ini adalah 802.3 (*Ethernet*), 802.11a/b/g/n MAC/LLC, 802.1Q(Vlan), ATM, CDP, HDP, FDDI, *Fiber Channel*, *Frame Relay*, HDLC, ISL, PPP, *Token Ring*, dan Q.921.

7. *Layer Physical*

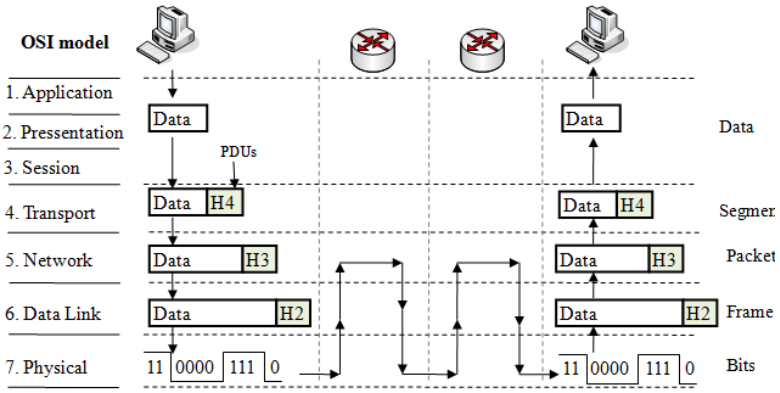
Layer paling bawah dalam model OSI. Layer ini berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan (kelistrikan/gelombang/medan), sinkronisasi bit, arsitektur jaringan (seperti halnya *ethernet* atau *token ring*), topologi jaringan dan pengakabelan. Selain itu, *level* ini juga mendefinisikan bagaimana NIC (*Network Interface Card*) dapat berinteraksi dengan media kabel atau gelombang radio.

Protokol yang berada dalam *layer* ini adalah RS-232, V.35, V.34, I430, I431, 802.11 a/b/g/n, *fiber optics, repeater, hub.*

2.2.3.1 Pengemasan Data

Pengemasan data (*Data Encapsulation*) proses pertama yang dilakukan sebelum pengiriman data melalui perangkat jaringan, berdasarkan OSI *layer* ketika sebuah *host* melakukan pengiriman data melalui jaringan ke *device* lainnya. Pada data akan ditambahkan *header* yang terdapat pada setiap OSI model. Proses komunikasi dan pertukaran informasi setiap layer menggunakan protokol yang disebut PDU (*Protocol Data Unit*) [5]. Proses enkapsulasi yang dilakukan oleh *sender* adalah sebagai berikut:

a. Informasi dari *user* diubah ke dalam bentuk data.
b. Data diubah ke dalam bentuk *segment* dan hubungan yang *reliable* dibentuk antara pengirim dan penerima.
c. *Segment* diubah ke dalam bentuk paket atau *datagram* dan sebuah alamat logika ditempatkan dalam *header* sehingga paket dapat diarahkan melalui antar jaringan.
d. Paket atau *datagram* diubah ke dalam bentuk *frame* untuk dikirimkan pada jaringan lokal. MAC *address* digunakan untuk menandai masing-masing *host* pada jaringan lokal.
e. *Frame* dirubah ke dalam *bit* dan *digital encoding* serta skema *clocking* digunakan.



Gambar 2.14 Proses Enkapsulasi dan Denkapsulasi

(*Sumber : http://wiki.mikrotik.com/wiki/Testwiki/Introduction_to_internetworking*)

Sebaliknya di *host* penerima akan melakukan proses denkapsulasi (pembongkaran *header* informasi) di setiap *layer* mulai dari bit sampai informasi yang diterima oleh *user* penerima.

2.2.4 Teknologi *Local Area Network*

Penggunaan jalur pada jaringan berdasarkan pada skema aliran data terdiri dari dua jenis, yaitu :

a. Contention

Pengiriman data dapat terjadi setelah jalur dalam keadaan kosong (tidak sedang digunakan). Jika terdapat dua *host* yang bersamaan menggunakan sebuah jalur maka pesan yang dikirimkan kemungkinan akan bertabrakan dan mengalami kerusakan (*collision)* [5].

b. Token Passing

Pengiriman dilakukan berdasarkan penerimaan sinyal token. Selama komputer hendak mengirimkan data belum menerima token, komputer tidak akan dapat menggunakan jalur sebagai media pengiriman data ke komputer lain [5]. Teknologi jaringan LAN (*Local Area Network*) terdiri dari beberapa jenis, yaitu :

1. Ethernet
2. Token Ring
3. FDDI

2.2.5 Pengalamatan Jaringan TCP/IP

Metode pengalamatan pada *layer* aplikasi disediakan oleh *host*, metode penamaan ini mengizinkan *host* untuk dikonfigurasi dengan nama yang mudah diingat. Sistem pengalamatan ini yang dapat langsung dilihat oleh pengguna.

Nomor *port* merupakan metode pengalamatan yang disediakan di layer *host to host.* Nomor ini digunakan untuk mengambarkan *interface* dari *software* yang akan memproses pada sebuah *host* [5].

IP *address* digunakan untuk metode pengalamatan *layer internet*. Saat ini banyak digunakan IP Versi 4, menggunakan 32 bit biner dan sistem bilangan yang digunakan adalah bilangan desimal [5].

MAC *address* merupakan metode pengalamatan di layer *network access*, Dikenal pula dengan istilah *hardware address.* Menggunakan 48 bit biner atau 12 digit *hexadecimal* [5].

Tabel 2.1 Metode Pengalamatan TCP/IP

Metode Pengalamatan Arsitektur TCP/IP	
Arsitektur TCP/IP	Metode Pengalamatan
Process/ Application	Nama Host (Host Name)
Host-to-Host	Nomor Port (Port Number)
Internet	Alamat IP (IP Address)
Network Access	Hardware Address (MAC Address)

(Sumber: Arifin Zaenal, Langkah Mudah Membangun Jaringan Kompuer. Penerbit ANDI,Yogyakarta 2005)

Diantara keempat metode pengalamatan di atas, metode pengalamatan TCP/IP yan sering digunakan yaitu IP *address.* Setiap *device* yang terhubung ke jaringan TCP/IP membutuhkan paling sedikit satu IP *address* yang bersifat unik, tidak boleh ada dua atau lebih IP *address* yang sama dalam satu jaringan. Sebuah alamat IP *address* terdiri dari dua bagian, yaitu :

a. Network ID

Network ID merupakan identitas alamat dari sebuah jalur. Semua *device* yang terhubung pada jalur fisik yang sama haris memiliki *network* ID yang sama. *Network* ID harus unik (tidak diperkenankan memberi alamat *network* ID yang sama pada jalur/*segment* yang berbeda).

b. Host ID

Host ID merupakan identitas bagi *host (workstation, server, interface router* dan *device* lain yang terhubung ke jaringan TCP/IP).

Dari sisi penggunaanya, alamat IP terbagi dalam dua jenis, yakni :

a. IP Private

IP *Address* yang digunakan pada jaringan privat tidak digunakan pada jaringan publik. IP *Address* yang termasuk dalam kelas tersebut, antara lain:

Tabel 2.2 Kelas IP Private

Kelas A	10	1-255	1-255	1-255
Kelas B	172	16-31	1-255	1-255
Kelas C	192	168	1-255	1-255

(Sumber: Arifin Zaenal, Langkah Mudah Membangun Jaringan Kompuer. Penerbit ANDI,Yogyakarta 2005)

b. IP Public

IP *Address* yang biasa digunakan pada jalur publik dan penggunaanya harus melalui proses registrasi dahulu. Alamat IP terbagi ke dalam lima kelas, yaitu A, B, C, D, dan E. Nilai pada oktet pertama menentukan kelas dari sebuah IP *Address*.

Tabel 2.3 Kelas IP Public

Kelas A	**1-126**	1-255	1-255	1-255
Kelas B	**128-191**	1-255	1-255	1-255
Kelas C	**192-223**	1-255	1-255	1-255
Kelas D	**224-239**	1-255	1-255	1-255
Kelas E	**240-255**	1-255	1-255	1-255

(Sumber: Arifin Zaenal, Langkah Mudah Membangun Jaringan Kompuer. Penerbit ANDI,Yogyakarta 2005)

2.2.6 Redudant Array Of Inexpensive Disk

Fault tolerant merupakan sebuah mekanisme yang dapat memilihkan kerusakan pada sistem yang sedang berjalan. Salah satu penerapan mekanisme *fault tolerant* pada *harddsik* yang didefinisikan sebagi sebuah RAID (*Redudant Array Of Inexpensive Disk)* [5].

RAID dapat diimplementasikan berbasis pada *software* ataupun *hardware.* Implementasi RAID berbasis pada *hardware* bergantung pada kemampuan *controller hard disk.* Biasanya selain memiliki kemampuan RAID, *vendor* akan menambahkan kemampuan *controller* tersebut dengan kemudahan dalam mengkonfigurasi RAID, menggunakan mekanisme *hot swap* sehingga *hard disk* dapat langsung dilepas dari *rack*-nya dan tidak perlu mesin terlebih dahulu dimatikan.

Berikut ini beberapa jenis RAID yang dapat diimpelementasikan pada *server*, diantaranya adalah [6] :

RAID 0

RAID 0 menggunakan dua atau lebih *hard disk* yang bertindak seolah-olah mereka satu *hard disk*. RAID 0 diibaratkan memiliki "0" perlindungan. Bahkan karena menggunakan dua *hard disk* maka memiliki dua kali risiko kehilangan data. Karena bila salah satu *drive* mengalami *error*, maka terancam kehilangan data.

Kelebihan:

1. RAID 0 menggunakan ruang *hard disk* secara maksimal karena tidak ada redundasi data.

2. RAID 0 memiliki kecepatan yang lebih karena lebih banyak ruang dari dua *hard disk* yang dijadikan satu.

Kekurangan:

1. Tidak ada perlindungan. Jadi jika kehilangan satu *hard disk* tunggal, data akan hilang.
2. Karena menggunakan dua *hard drive* tanpa redundansi, maka resiko jadi dua kali lipat. Makanya akan lebih aman untuk menyimpan data dalam *hard disk* tunggal, misalnya bila menyimpan *file* 10 MB dimana masing-masing *drive* menerima 5 MB, maka jika salah satu *drive* rusak, hanya kehilangan data 5 MB.



Gambar 2.15 Implementasi RAID 0

(*Sumber: http://mediabisnisonline.com/mengenal-komponen-server-tipe-RAID-dan-tingkatannya)*

RAID 1

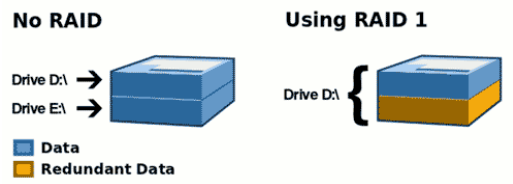
Dalam RAID 1 terjadi *mirrorring* antar *hard disk*. Sehingga dia menyediakan redundansi jika salah satu *disk* mengalami *error*. Tidak seperti RAID 0 di mana semua *space* digabungkan, RAID 1 hanya menggunakan setengah ruang karena *drive* kedua digunakan untuk redundansi. Dengan syarat kedua *hard drive* ukurannya harus sama.

Kelebihan :

Redundansi dan Kecepatan.

Kekurangan :

Space hard disk tidak digunakan secara efisien. Karena kedua *hard disk* adalah salinan satu sama lain, hanya setengah dari ukuran jumlah gabungan yang digunakan.



Gambar 2.16 Implementasi RAID 1

(*Sumber: http://mediabisnisonline.com/mengenal-komponen-server-tipe-RAID-dan-tingkatannya)*

RAID 5

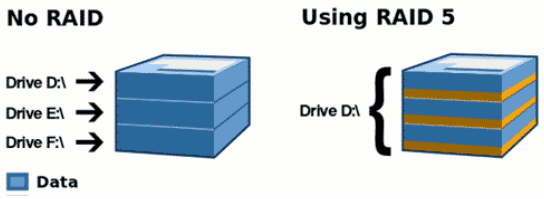
RAID 5 adalah *level* yang paling populer digunakan di *server* saat ini. Dengan RAID 5 bisa memiliki performa dan efisiensi penggunaan ruang. Dalam RAID 5 redundansi didistribusikan di antara semua *drive*. Jumlah minimum dari *drive* yang dapat digunakan pada RAID 5 adalah tiga.

Kelebihan :

1. Efisiensi penggunaan kombinasi *hard disk.*
2. Toleransi kesalahan, jika salah satu *hard disk down/error* maka data tetap aman.

Kekurangan :

1. Kecepatan RAID 5 tidak secepat RAID 0 atau 1.
2. Jika lebih dari satu *hard disk* mengalami *error*, maka data terancam hilang.



Gambar 2.17 Implementasi RAID 5

(*Sumber: http://mediabisnisonline.com/mengenal-komponen-server-tipe-RAID-dan-tingkatannya)*

RAID 6

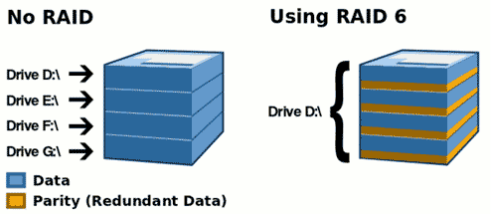
RAID 6 pada dasarnya sama dengan RAID 5, dengan perbedaan dua *drive* bisa *down* pada saat yang sama bukan hanya satu. Jumlah minimum dari *drive* yang dapat digunakan dengan RAID 6 adalah empat.

Kelebihan :

Meskipun dua *hard disk* mengalami *down* bersamaan, data akan tetap aman.

Kekurangan :

1. *Space* total *hard drive* sangat berkurang karena lebih banyak dialokasikan untuk partisi redundansi.
2. Kecepatan RAID 6 tidak secepat RAID 0 atau 1.
3. Proses *rebuilt* lebih lambat. Ketika *drive down*, maka perlu *rebuilt* kembali. Kinerja akan menurun jauh bila dibandingkan dengan metode RAID lainnya.



Gambar 2.18 Implementasi RAID 6

(*Sumber: http://mediabisnisonline.com/mengenal-komponen-server-tipe-RAID-dan-tingkatannya)*

RAID-Z

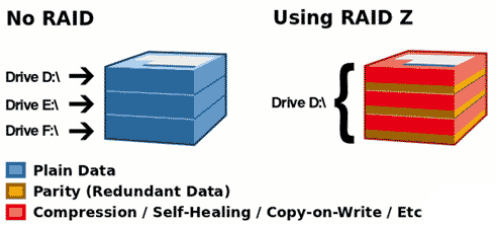
RAID-Z dan RAID-Z2 adalah penemuan *Sun Micro System*. RAID-Z memiliki semua manfaat dari RAID 5 dan fitur lainnya yang membuatnya jauh lebih unggul. Seperti dengan RAID 5, RAID Z dapat mendukung sejumlah *hard disk* yang bekerja sama dan satu *disk* untuk redudansi. Jumlah minimum dari *hard disk* adalah tiga dan hanya satu yang bisa *down* pada suatu waktu. Jika lebih dari satu *hard disk* rusak pada saat yang sama, maka beresiko kehilangan data.

Kelebihan :

Memiliki semua kelebihan dari RAID 5 dan fitur lainnya.

Kekurangan :

Hanya dapat digunakan dengan sistem operasi berbasis Open Solaris seperti Nexenta dan atau sistem berbasis BSD seperti FreeBSD.



Gambar 2.19 Implementasi RAID-Z

(*Sumber: http://mediabisnisonline.com/mengenal-komponen-server-tipe-RAID-dan-tingkatannya)*

RAID Z2

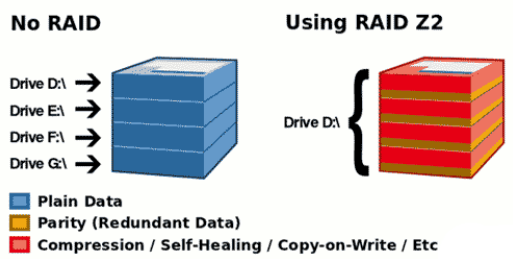
RAID Z2 hampir identik dengan RAID Z dan mirip dengan RAID 6. Dalam RAID Z2, meski dua *hard disk* bisa down di waktu bersamaan namun data akan tetap aman dan mudah diakses. Sama seperti RAID Z, RAID Z2 jauh lebih unggul dengan RAID 6 karena di dalamnya terdapat banyak fitur lainnya. Jumlah minimum *drive* untuk menggunakan RAID Z2 adalah empat.

Kelebihan :

1. Data lebih aman meski dua *drive* bisa *down* pada saat yang sama bukan hanya satu.
2. Memiliki semua manfaat dari RAID Z.

Kekurangan :

1. Dua *hard disk* digunakan untuk paritas, sehingga ukuran jumlah gabungan *space* sangat terbatas.
2. Hanya dapat digunakan dengan sistem operasi berbasis Open Solaris seperti Nexenta dan atau sistem berbasis BSD seperti FreeBSD.



Gambar 2.20 Implementasi RAID-Z2

(*Sumber: http://mediabisnisonline.com/mengenal-komponen-server-tipe-RAID-dan-tingkatannya)*

2.2.7 File System

Berikut ini adalah *file system* yang terdapat pada sistem operasi berbasis UNIX, yaitu :

2.2.7.1 *Zetta File System*

Zetta file system (ZFS) adalah kombinasi *file system* dan *logical volume manager* yang didesain oleh *Sun Microsystem.* Fitur ZFS meliputi perlindungan terhadap kerusakan data (*data corruption)* yang mendukung kapasitas penyimpanan yang tinggi, efesiensi kompresi data, integrasi antara *file sistem* dan *volume management, snapshot,* dan *copy-on-write* kloning, perbaikan otomatis dan pengecekan integritas data berkelanjutan, RAID-Z dan Native NFSv4 ACLs.

ZFS menjamin integritas melalui penggunaan *fletecher-based checksum* atau SHA-256 *hash* melalui *file system tree.* Setiap *block* data dilakukan proses *cheksummed* dan nilai tersebut disimpan di pointer block data daripada disimpan pada blok itu sendiri. ZFS menyimpan *checksum* pada setiap blok yang berada di *parent-block pointer* sehingga seluruh *pool* tervalidasi.

ZFS menggunakan *copy-on-write transactional object model.* Semua *block pointer* di dalam *file system* memiliki 256 bit *checksum* atau *hash* (*Fletche*r-2, *Fletcher*-4, atau SHA-256) dari blok target, yang diverifikasi ketika blok dibaca. Blok yang berisi data aktif tidak pernah ditimpa, melainkan sebuah blok baru di alokasikan, dan data yang dimodifikasi ditulis disini. Untuk mengurangi *overhead* ketika proses ini, maka *multiple update* akan digrup menjadi grup *transactional* dan ZIL menulis *cache* data digunakan ketika sinkronisasi penulisan secara semantik dibutuhkan. Blok data disusun ke dalam sebuah *tree* yang menjadi hirarki alokasi penyimpanan *checksum* [11].

2.2.7.2 *Unix File System*

UFS (*Unix File System*), *file system* yang juga sering disebut sebagai *Berkeley Fast File System* merupakan *file system* yang banyak digunakan pada lingkungan sistem operasi Unix dengan dukungan penyimpanan hingga 8 ZB.

2.2.8 Teknologi *Storage Server*

Terdapat banyak faktor penting untuk diperhatikan dalam melakukan desain dan implementasi sistem *storage*, diantaranya adalah [17]:

a. Capacity

Karena jumlah data digital kian lama kian meningkat, maka faktor kapasitas menjadi poin yang paling utama dalam memenuhi kebutuhan *storage* saat ini. Menurut sebuah survei, pertumbuhan kebutuhan kapasitas penyimpanan data pada sebuah perusahaan berkembang melampaui apa yang dinyatakan dalam hukum *moore*, yaitu perkembangannya melebihi dua kali lipat dalam 18 waktu bulan.

b. Performance

Performa yang hebat juga harus diperhatikan dalam memilih dan menggunakan sistem *storage* data. Kecepatan dan kemampuan membaca dari perangkat *storage* tersebut harus seimbang dengan perkembangan yang terjadi pada perangkat yang menggunakannya. *Bandwidth* untuk menghantarkan data dari media *storage* harus sesuai dengan kecepatan proses dari komputer yang menggunakannya, harus sesuai dengan performa jaringan komunikasi data yang akan dilewatinya, dan harus sesuai dengan aplikasi yang mengaksesnya seperti misalnya aplikasi multimedia.

c. Availability

Karena semakin besarnya ketergantungan masyarakat terhadap data digital, maka ketersediaan dan reliabilitas dari media penyimpanannya juga harus benar-benar diperhatikan dan ditingkatkan. Hal ini menjadi sangat penting untuk menghindari terjadinya kehilangan isi dari data dan kehilangan kesempatan mengakses data yang tersimpan di dalamnya. Maka dari itu, media *storage* yang memiliki ketersediaan dan reliabilitas tinggi sudah barang tentu dibutuhkan untuk mencegah terjadinya kesulitan mengakses data. Selain itu, sistem *storage* juga harus memiliki sistem penyelamatan data ketika terjadi bencana, seperti misalnya memiliki sistem *mirroring* atau teknik *back-up* yang dapat meng-*copy* data yang disimpannya ke lokasi-lokasi yang berbeda.

d. Scalability

Solusi penyimpanan data yang dimiliki idealnya tidak hanya dapat memenuhi kebutuhan saat ini saja, melainkan dapat juga mengatasi perkembangan kebutuhan di masa yang akan datang. Sistem penyimpanan ini hendaknya dapat berkembang dengan mudah seiring dengan berkembangnya kebutuhan akan penyimpanan.

e. Cost

Media storage yang tentu dipasang dalam kapasitas yang sangat besar hendaknya harus juga memiliki harga yang tidak terlalu memberatkan penggunanya. Hal ini dikarenakan pengguna pasti akan terus membutuhkan media penyimpanan selama datanya masih ingin disimpan, maka itu dengan harga media penyimpanan yang murah, pengguna tidak akan lepas dari penggunaan media tersebut. Harga sistem penyimpanan yang murah sebaiknya bukan hanya dari segi perangkat kerasnya saja, namun juga termasuk murah dalam *maintenance* dan manajemen dari sistem *storag*e tersebut.

Dengan didorong oleh faktor-faktor di atas, bermunculanlah perkembangan teknologi sistem *storage* yang bertujuan untuk memenuhi semua kebutuhan tersebut. Teknologi *networking* akhirnya diadopsi menjadi sebuah sistem *storage* yang mampu melayani penyimpanan data dalam skala *enterprise*. Saat ini telah tersedia beragam jenis teknologi *storage server,* teknologi tersebut adalah DAS (*Direct Attached Storage*), SAN (*Storage Area Network*), dan NAS (*Network Attached Storage*).

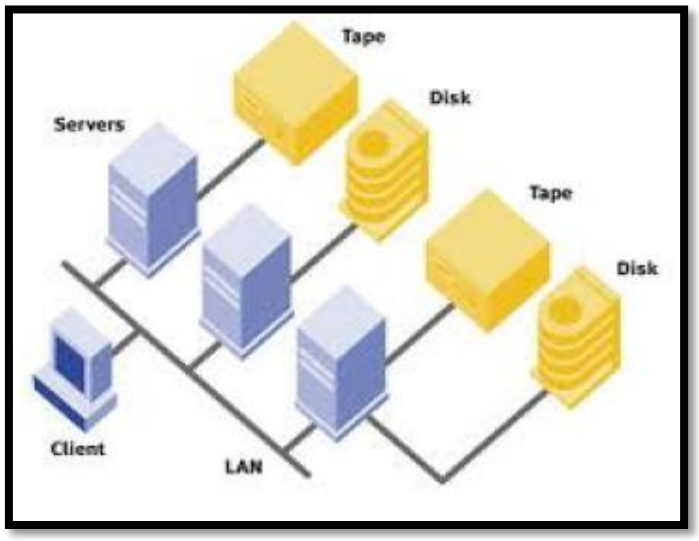
Berikut ini adalah penjelasan dari perbedaan ketiga teknologi *storage server* tersebut, yaitu :

2.2.8.1 *Direct Attached Storage*

DAS (*Direct Attaches Storage*) merupakan sebuah istilah yang menjelaskan perangkat penyimpanan (*storage)* yang secara langsung ditempelkan pada komputer itu sendiri. Sistem DAS banyak ditemukan di *server-server, stand alone* PC, dan *workstation*.

Konfigurasi DAS yang umumnya terjadi adalah terdiri dari sebuah komputer yang terkoneksi secara langsung dengan satu atau lebih *hard disk* atau *disk array.* Dengan kata lain, PC atau perangkat komputer langdung dipasang satu atau lebih hard disk yang dapat diakses secara langsung untuk menyimpan dan membuka data.

Jalur komunikasi yang digunakan antara PC dengan media penyimpanan ini adalah dengan sistem standar *bus* yang digunakan untuk mengkoneksikan antara *hard disk* dengan sistem komputer, seperti SCSI, ATA, Serial ATA (SATA), dan *Fiber Channel* (FC).



Gambar 2.21 Direct Attached Storage Pada Jaringan LAN

(*Sumber : http://yuwaka.blogspot.com/2013/12/solusi-penyimpanan-data-untuk-perusahaan.html*)

2.2.8.2 *Storage Area Network*

SAN (*Storage Area Network*) adalah sebuah jaringan berkecepatan sangat tinggi yang khusus, terdiri dari *server* dan *storage*. Terpisah dan berbeda dengan LAN/WAN perusahaan, tujuan utama SAN adalah untuk menangani trafik data dalam jumlah besar antara *server* dan peralatan penyimpan, tanpa mengurangi *bandwidth* yang ada di LAN/WAN. Biasanya tersambung melalui *fiber channel*, sebuah teknologi komunikasi data berkecepatan sangat tinggi, menjadikan SAN sebuah jaringan *dedicated* yang *platform-independent* yang beroperasi dibelakang *server* [17].

SAN terdiri dari infrastruktur komunikasi, yang memberikan sambungan fisik, dan lapisan manajemen, yang mengatur sambungan, elemen penyimpan, dan sistem komputer sehingga menghasilkan *transfer* data yang sangat aman dan handal. SAN merupakan solusi konfigurasi masa depan untuk media penyimpanan data dalam jumlah besar dengan berbagai layanan yang berbasis *online* di internet maupun intranet. Keuntungan utama dari SAN adalah:

a. Availability

Satu *copy* dapat diakses oleh semua *host* melalui jalur yang berbeda dan semua data lebih efisien dalam mengelolanya.

b. Reliability

Infrastruktur *transport* data yang dapat menjamin tingkat kesalahan yang sangat minimal, dan kemampuan dalam mengatasi kegagalan.

c. Scalability

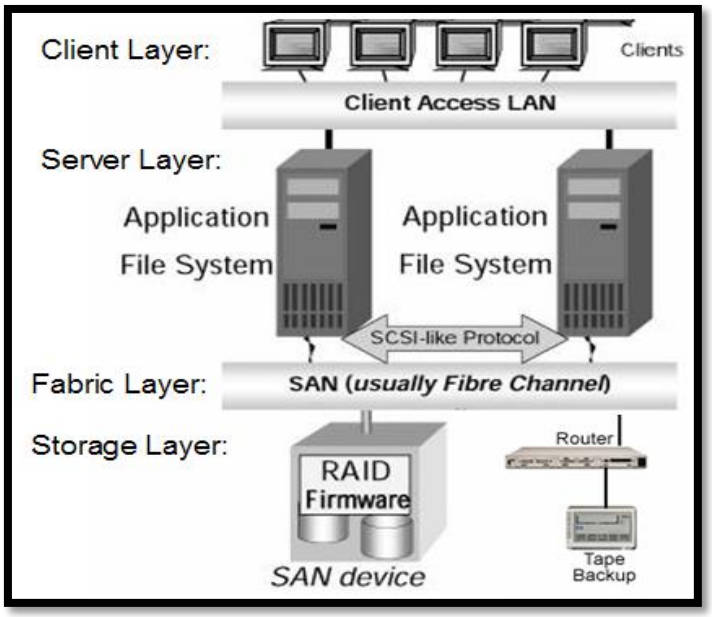
Server maupun media penyimpanan (*storage*) dapat ditambahkan secara *independent* satu dan lainnya dengan tanpa pembatas harus menggunakan sistem yang *proprietary*.

d. Performance

Fiber channel mempunyai bandwidth 100 Mbps *bandwidth* dengan *overhead* yang rendah, dan SAN akan memisahkan trafik *backup* dengan trafik standar LAN/WAN.

e. *Managability*

Berkembangnya perangkat lunak dan standar baik utk FC-AL (*Fiber Channel Arbitrated Loop*) maupun *Fiber channel fabric* memungkinkan pengelolaan dilakukan secara terpusat dan koreksi dan deteksi kesalahan yang pro-aktif.



Gambar 2.22 Arsitektur Storage Area Network

(*Sumber : http://yuwaka.blogspot.com/2013/12/solusi-penyimpanan-data-untuk-perusahaan.html*)

2.2.8.3 *Network Attached Storage*

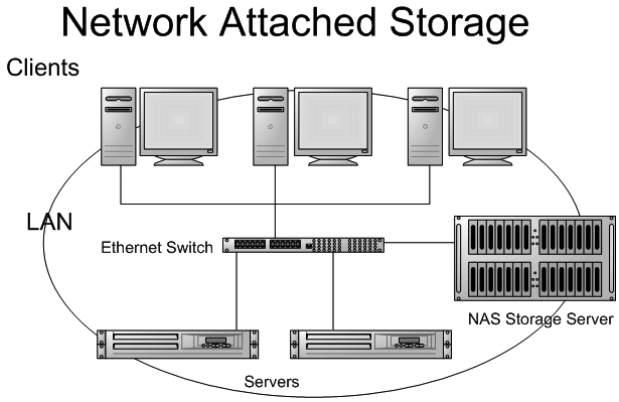
Network Attached Storage (NAS) adalah sebuah *server* dengan sistem operasi yang dikhususkan untuk melayani kebutuhan berkas data. NAS berbeda dengan *server* pada umumnya, yaitu NAS hanya dapat digunakan untuk *data storage* [7].

NAS (*Network Attached Storage)* pertama kali dikenalkan oleh *Sun Microsystem* yang mengembangkan sistem operasi Unix yang digunakan sebagai *file server* menggunakan NFS (*Network File System)* dan telah diimplementasikan dengan berbagai versi untuk mengakomodasi kebutuhan layanan data di *platform* Unix/Linux.

CIFS (*Common Internet File System)* merupakan layanan *file server* yang dulunya disebut sebagai SMB (*Server Message Block)* juga telah dikembangkan oleh perusahaan ini untuk mengakomodasi kebutuhan data di *platform* Windows.

Untuk mengakses data pada *server,* NAS mendukung berbagai akses protokol dan mengizinkan *host* dengan platform Windows, Apple OS X, dan Unix terkoneksi dan menggunakan data pada *server*.

NAS normalnya memiliki satu atau lebih *hard disk,* dan *hard disk* tersebut dikombinasikan untuk membuat area *storage* yang digunakan untuk *redudancy.* Hal ini digunakan untuk mengatasi kesalahan pada *storage,* Jika *hard disk* gagal kemudian sistem akan tetap bekerja dan data tidak hilang.



Gambar 2.23 Skema Implementasi Network Attached Storage

(*Sumber: http://www.tech-faq.com/network-attached-storage.html)*

NAS memiliki beberapa kelebihan daripada tradisional *file server,* yaitu :

a. NAS memiliki keamanan yang lebih baik sebagai *server* dengan *dedicated operating system* untuk menyediakan data, tidak ada *service* lain yang bekerja seperti *mail server,* DHCP *server,* DNS *server,* dll.
b. NAS didesain untuk menangani *high avaibality,* hal ini ditunjukan dengan adanya mekanisme redudansi pada *storage* dan mengizinkan *hardware* mengalami kesalahan tanpa menghilangkan data berharga.
c. NAS mudah digunakan dan dikelola karena menyediakan *interface* yang dapat diakses melalui *web browser* dan mendukung *remote access* untuk dapat di akses darimanapun selama masih dalam satu *network.*
d. NAS dapat bekerja pada lingkungan jaringan yang heterogen. Oleh karena itu, NAS sangat *lower cost* dibandingkan dengan tradisional *server* selama penggunaan untuk perluasan dan penambahan ketersedian data serta keamanan.

Sistem operasi NAS banyak dibangun di beberapa sistem operasi berbasis Unix dan Linux. Berikut adalah beberapa sistem operasi *open source* berbasis NAS, yaitu :

a. FreeNAS

FreeNAS adalah *embeded operating system* yang memiliki lisensi publik (*open source)* berbasis BSD/Unix yang menjalankan fungsi sebagai NAS (*Network Attached Storage)* dan mendukung koneksi berbagai *platform* sistem operasi seperti Windows, Apple OS X, Linux dan Unix [7].

FreeNAS dapat diinstal pada USB *flash drive* atau *hard drive* dengan kebutuhan *space* minimal 32 MB. FreeNAS mendukung berbagai fitur untuk menyediakan data / *storage* pada jaringan komputer, sistem operasi ini mendukung *Windows Machine* menggunakan CIFS (*Common Internet File System)* protokol untuk mengakses *file* pada jaringan, CIFS juga mendukung berbagi *file* pada lingkungan *platform* Linux dan Apple OS X.

Selain CIFS, terdapat protokol NFS (*Network File System)* yang sudah lama digunakan untuk berbagi *file* pada lingkungan *platform* Unix. FTP (*File Transfer Protocol*) juga telah didukung oleh sistem operasi ini untuk mendukung berbagi *file* di berbagai *platform* sistem operasi. FreeNAS mendukung berbagai bentuk redudansi *storage* seperti RAID 0, 1, Z dan Z2.

Sementara itu untuk *file system*, NAS memiliki dua ungulan *file system* yang sering digunakan, yaitu UFS (*Unix File System*) dan ZFS (*Zetta File System)*. Salah satu unggulan *file system* yang baru terdapat pada FreeNAS yaitu ZFS, dikarenakan memiliki fitur *snapshot* dan *replication* yang digunakan untuk proteksi data dan *data recovery*.

b. NAS4Free

NAS4Free adalah sebuah distribusi *embedded open source* NAS (*Network-Attached Storage*) menggunakan FreeBSD sebagai landasan. NAS4Free mendukung *sharing data* lintas berbagai sistem operasi, termasuk Windows, Apple dan Linux.

NAS4Free mudah dikonfigurasi untuk digunakan di lingkungan rumah dan perusahan, disamping kemampuan untuk mengelola dan berbagi data lintas jaringan dalam jumlah yang besar. NAS4Free juga dibekali banyak fitur yang menyokong aneka *streaming* untuk berbagi konten multimedia dengan perangkat lainnya dalam jaringan. NAS4Free menyertakan *software* termasuk ZFS v28 (RAIDZ, RAIDZ2 dan RAIDZ3),

RAID (0,1,5), *Disk Encryption*, S.M.A.R.T / *Email Reports*, dan mendukung sejumlah protokol seperti: CIFS, FTP, NFS, TFTP, AFP, RSYNC, Unison, iSCSI, HAST, CARP, *Bridge*, UPnP, dan BitTorrent, dan diklaim semuanya mudah dikonfigurasi via *web interface* [8].

c. OpenFiler

OpenFiler adalah sebuah sistem operasi pengelola penyimpanan data. OpenFiler memanfaatkan paket-paket aplikasi *open source* lainnya seperti *Apache*, *Samba*, *Linux Volume Management*, ext3, Linux NFS dan iSCSI yang semuanya ditargetkan untuk pengguna *enterprise*.

OpenFiler menggabungkan teknologi *open source* tersebut menjadi solusi yang baik dengan *frontend* dan GUI berbasis *web* yang mudah diatur. OpenFiler dapat digunakan sebagai basis untuk membangun NAS (*Network Attached Storage*) dan perangkat SAN (*Storage Area Network*).

OpenFiler dibangun diatas sistem operasi Centos Linux dan mendukung protokol jaringan termasuk NFS, SMB/CIFS, HTTP/WebDAV dan FTP. Direktori jaringan yang didukung OpenFiler antara lain NIS, LDAP (berikut dukungan untuk SMB/CIFS *encrypted passwords*), *Active Directory* dan *Hesiod*. Protokol autentifikasi termasuk Kerberos 5 [9].

2.2.9 Parameter Kinerja Jaringan

Kriteria penting dari sudut pandang pemakai jaringan adalah keandalan, yaitu kriteria pengukuran seberapa mudah suatu sistem terkena gangguan, terjadi kegagalan atau berpoperasi secara tidak benar [10].

Keandalan adalah ukuran statistik kualitas komponen dengan menggunakan strategi pemeliharaan, kualitas redundansi, perluasan jaringan secara geometris dan kecenderungan statis dalam merasakan sesuatu secara tidak langsung tentang bagaimana suatu paket ditransmisikan oleh sistem tersebut. Kinerja jaringan dapat diukur berdasarkan kriteria, yaitu :

a. Kriteria *level* pemakaian yaitu waktu respon dan keandalan.
    1. Waktu respon yaitu tanggapan saat paket dipancarkan dengan benar.
    2. Keandalan yaitu suatu keandalan yang dapat menentukan seberapa berfungsinya sistem pada suatu tugas pengiriman paket.
b. Kriteria *level* jaringan, yaitu waktu respon rata-rata. Penentuan waktu respon rata-rata yang dilakukan dengan dua langkah, yaitu :
    1. Menentukan rata-rata penundaan satu jalur paket melewati jaringan dan antar mukanya sebagai suatu fungsi beban terhadap ukuran paket.
    2. Menggunakan informasi dengan penundaan dan pemakaian link untuk menghitung waktu respon rata-rata pemakai.
c. Kriteria kinerja khusus, yaitu daya kerja dan penundaan rata-rata.

2.2.10 Manajemen Ketersediaan

Manajemen ketersediaan (*Avaibality Management)* data memungkinkan organisasi ketersediaan layananan teknologi informasi dalam rangka menunjang bisnis sesuai biaya yang dianggarkan. Dengan aktifitas layanan yang tinggi menyadari akan kebutuhan ketersediaan, penyusunan rencana ketersediaan, memonitor ketersediaan, dan kewajiban memonitor pemeliharaan [10].

Ketersediaan (*Avaibality*) adalah kemampuan dari sebuah komponen teknologi informasi untuk menyelenggarakan layanan yang disepakati selama jangka waktu tertentu atau pada saat dibutuhkan. Rumus untuk menghitung ketersediaan data (*Avaibality*), yaitu :

$$AV\ (\%) = (AST\text{-}DT)/AST\ X\ 100\%$$

Keterangan :

AST = *Agreed Service Time*

DT = *Down Time*

Menurut publikasi ITIL v3, proses di dalam manajemen ketersediaan mempunyai dua elemen utama yaitu :

a. *Reactive Activities*, apsek reaktif dari pengelolaan ketersediaan layanan melibatkan aktifitas pemantauan (*monitoring),* pengukuran (*measurement),* analisa, dan manajemen keseluruhan kejadian insiden masalah terkait hilangnya ketersediaan.

b. *Proactive Activities,* melibatkan aktifitas perencanaan, desain dan usaha-usaha peningkatan ketersediaan. Aktifitas tersebut pada prinsipnya terkait dengan perencanaan desain.

2.2.11 Reactive Activities

Kegiatan yang dilakukan berdasarkan *reactive activities* adalah [10] :

2.2.11.1 *Monitoring*

Monitoring atau pemantauan dilakukan pada layanan jaringan menggunakan aplikasi PRTG (*Paessler Router Traffic Grapher*). Aplikasi PRTG digunakan untuk memantau jaringan secara periodik. Dan untuk mendukung aplikasi ini dilakukan aktivasi fungsi SNMP *service* dari masing-masing peralatan baik *switch* dan *router.*

Sedangkan paket *ping* dan NMS (*Network Management Service*) digunakan untuk memeriksa aktifitas jaringan berbasis teknologi TCP/IP (*Transmission Control Protocol/Internet Protocol*).

2.2.11.2 Pengukuran

Kualitas koneksi jaringan dapat dilihat melalui nilai parameter kinerja sebagai berikut ini :

a. Throughput

Throghput adalah kecepatan (*rate*) *transfer* data efektif, yang diukur dalam bps. *Throughput* merupakan jumlah total kedatangan paket yang sukses yang diamati pada *destination* selama interval waktu tersebut.

$$Throughput = \frac{Paket\ data\ yang\ diterima}{Lama\ pengamatan}$$

Throughput yang diperoleh pada saat melakukan pengiriman paket, bergantung pada :

1. Kepadatan *traffic* jaringan.
2. Besar paket yang ditransmisikan.
3. *Receive* dan *send* TCP *windows host* yang melakukan pertukaran data.

b. *Delay/Latency*

Delay/*Latency* didefinisikan sebagai total waktu tunda suatu paket yang diakibatkan oleh proses transmisi dari satu titik ke titik lain yang menjadi tujuannya. *Delay* dalam jaringan dapat digolongkan sebagai berikut *delay processing, delay packetization, delay serialization, delay jitter buffer,* dan *delay network.*

$$\textit{Delay rata-rata} = \frac{\textit{Total delay}}{\textit{Total paket yang diterima}}$$

c. *Jitter*

Jitter didefinisikan sebagai variasi dari *delay* atau variasi waktu kedatangan paket. Banyak hal yang dapat menyebabkan *jitter*, diantaranya adalah peningkatan trafik secara tiba-tiba sehingga menyebabkan penyempitan *bandwith* dan menimbulkan antrian.

$$\textit{Jitter} = \frac{\textit{Total variasi delay}}{\textit{Total paket yang diterima-1}}$$

d. *Packet Loss*

Packet loss adalah perbandingan seluruh paket IP yang hilang dengan seluruh paket IP yang dikirimkan antara pada *source* dan *destination*. Salah satu penyebab paket *loss* adalah antrian yang melebihi kapasitas *buffer* pada setiap *node*.

$$\textit{Paket loss} = \frac{\textit{Paket data yang dikirim} - \textit{paket data yang diterima}}{\textit{Paket data yang dikirim}} \text{ X } 100\%$$

2.2.12 Aplikasi

Berikut adalah beberapa aplikasi yang digunakan untuk *vulnerability scanning*, *cloud*, *simulation*, *monitoring* dan mengukur *quality of service* suatu jaringan komputer, yaitu :

2.2.12.1 Nessus

Nessus adalah salah satu *scanner* keamanan jaringan yang harus digunakan oleh *administrator system* untuk melakukan *software scanning* yang dapat digunakan untuk meng-audit kemanan sebuah sistem, seperti *vulnerability*, *misconfiguration*, *security*

patch yang belum diaplikasikan, *default password*, dan *denial of service.* Nessus berfungsi untuk *monitoring* lalu-lintas jaringan.

Dikarenakan fungsi dari Nessus dapat digunakan untuk mendeteksi adanya kelemahan ataupun cacat dari suatu sistem maka Nessus menjadi salah satu *tool* andalan ketika melakukan audit keamanan suatu sistem. Nessus dapat digunakan untuk melakukan audit sebagai berikut :

1. *Credential* dan *un-credential port scanning.*
2. *Vulnerability scanning* pada jaringan komputer.
3. *Credential based patch* audit pada sistem operasi Windows dan Unix.
4. Audit konfigurasi SQL *database.*
5. Pengujian anti-virus yang terpasang.
6. *Software enumeration* pada sistem operasi berbasis Windows dan Unix.
7. Pengujian *vulnerability* pada aplikasi berbasis *web*, dll.



Gambar 2.24 Logo Aplikasi Nessus

(*Sumber: https://sathisharthars.wordpress.com/2014/03/14/installing-nessus-in-kali-linux-1-0-6/*)

2.2.12.2 OwnCloud

OwnCloud adalah aplikasi *open source* yang digunakan untuk membangun sebuah komputasi awan pribadi. Diantara sejumlah peningkatan yang disertakan OwnCloud adalah fitur sinkronisasi berkas (*file synchronization*), fitur berbagi berkas (*file sharing*), dan integrasi layanan *cloud storage* eksternal [12].



Gambar 2.25 Logo Aplikasi OwnCloud

(*Sumber: https://blog.docker.com/2015/07/official-repos-kibana-owncloud-arangodb-kaazing//*)

OwnCloud dibangun menggunakan bahasa pemrogaraman PHP 5, aplikasi ini dapat melakukan sinkronisasi lebih cepat dan dengan mudah dapat disambungkan ke layanan *cloud* eksternal seperti Amazon S3, Dropbox, Google Drive atau Strato Hidrive.

OwnCloud juga secara otomatis dapat didaftarkan pada WebDAV, IMAP, Samba, dan FTP, apabila telah tercantum dalam daftar konfigurasi OwnCloud. Pengguna OwnCloud dapat menentukan siapa saja yang memiliki hak akses yang dibatasi berdasarkan jangka waktu yang dapat ditentukan seperti untuk membaca, mengubah, dan menghapus *file* yang terbagi. Termasuk kemungkinan untuk menambahkan perlindungan *password* pada URL di berkas yang dibagikan.

2.2.12.3 Vmware Workstation

Vmware Workstation adalah sebuah perangkat lunak mesin virtual untuk arsitektur komputer x86 dan x86-64. Perangkat lunak ini digunakan untuk membuat banyak x86 dan x86-64 komputer virtual dan digunakan secara simultan dengan sistem operasi yang digunakan. Setiap mesin virtual tersebut bisa menjalankan sistem operasi yang dipilih, seperti Windows, Linux, varian BSD dan lain sebagainya.

Dalam arti yang sederhana, Vmware Workstation bisa menjalankan banyak sistem operasi secara simulatan dengan menggunakan satu fisik mesin. [16].



Gambar 2.26 Logo Aplikasi Vmware

(*Sumber: http://www.kolmisoft.com/softswitch/try-mor/mor-free-version/mor-vmware*)

2.2.12.4 Paessler Router Traffic Grapher

PRTG (*Paessler Router Traffic Grapher)* adalah perangkat lunak pemantauan *bandwidth* dan banyak parameter jaringan lain melalui SNMP, *packet sniffing*, atau *Cisco NetFlow* yang memungkinkan untuk pengukuran *traffic* berdasarkan alamat IP dan protokol [13].

Pengukuran berbasis SNMP hanya berbasis pada *port*. *Software* ini juga memungkinkan untuk secara cepat mempersiapkan dan menjalankan sebuah proses pemantauan untuk sebuah jaringan tertentu, dengan PRTG ini maka dengan mudah dapat mengetahui sejumlah data yang mengalir melalui perangkat seperti *router* dan memantau penggunaan PC serta menganalisa *traffic* yang dapat dikategorikan ke dalam beberapa jenis protokol.



Gambar 2.27 Logo Aplikasi PRTG

(*Sumber: http://community.spiceworks.com/product/15779-paessler-prtg-network-monitor*)

PRTG berjalan pada mesin Windows di dalam jaringan selama 24 jam setiap hari dan terus menerus mencatat penggunaan parameter jaringan. Dengan PRTG ini dapat memantau semua aspek jenis protokol mulai dari jenis jaringan protokol FTP, HTTP, HTTPS, SMTP, ICMP, DNS, POP3, SNMP dan lainnya.

Berikut ini fitur – fitur dasar yang dimiliki PRTG, yaitu :

a. Kemampuan untuk melakukan *monitoring* pada jaringan yang digunakan oleh lebih dari 80.000 *user* setiap harinya.
b. Pengumpulan data dapat melalui SNMP, Packet Sniffing, dan NetFlow.
c. Mengklasifikasi *traffic* jaringan ke dalam parameter-parameter seperti IP *Address*, protokol, dll.
d. Dapat bekerja dengan perangkat jaringan seperti *switch, router, firewall,*dll.

2.2.12.5 Wireshark

WireShark adalah perangkat lunak *open source* yang digunakan untuk menganalisis jaringan yang biasa digunakan oleh *network administrator* untuk menganalisa kinerja jaringan termasuk protokol di dalamnya [14]. Tujuan dari *monitoring* dengan Wireshark adalah :

a) Memecahkan masalah jaringan.
b) Memerikasa keamanan jaringan.
c) Men-*debug* implementasi protokol.
d) Mempelajari protokol jaringan internal.

Wireshark ini memiliki beberapa keuntungan, diantaranya dapat memantau paket paket data yang diterima dari internet. Wireshark ini bekerja pada *layer* aplikasi, yaitu layer terakhir dari OSI *layer*. Dengan menggunakan protokol pada *layer* aplikasi seperti HTTP, FTP, TELNET, SMTP, DNS, *administrator* dengan mudah memonitor jaringan yang ada.



Gambar 2.28 Logo Aplikasi Wireshark

(*Sumber: http://knowledgepia.com/en/k-blog/security/wireshark*)

2.2.12.6 Diskboss

Diskboss adalah sebuah perangkat lunak manajemen *file* dan *disk* yang membantu *user* untuk mencari dan mengklasifikasikan *file*, melakukan analisis pemanfaatan ruang *disk*, mendeteksi dan menghapus *file* duplikat, mengatur *file* sesuai dengan aturan dan kebijakan yang ditetapkan oleh *user*, menyalin sejumlah besar *file*, sinkronisasi *disk* dan direktori, serta pembersihan ruang *disk* yang terbuang percuma, dll [15].



Gambar 2.29 Aplikasi Diskboss

(*Sumber: https://downfullsoft.wordpress.com/tag/diskboss-ultimate-license-code/*)

2.2.12.7 Filezilla

FileZilla adalah perangkat lunak *open source* yang berguna untuk *transfer file* via protokol FTP di jaringan komputer atau internet. FileZilla dapat dijalankan di sistem operasi Windows XP, Windows Vista, Windows 7, Linux dan Mac OS. Fitur utama FileZilla, yaitu *site manager*, *message log*, *file* dan *folder view*, dan *transfer queue* [18].



Gambar 2.30 Logo Aplikasi Filezilla

(*Sumber: https://commons.wikimedia.org/wiki/File:FileZilla_logo.svg*