

BAB II

LANDASAN TEORI

2.1 Pengertian Jaringan Komputer

Pengertian jaringan komputer adalah sebuah system operasi yang terdiri dari beberapa komputer dan perangkat jaringan lainnya yang bekerja sama dalam mencapai suatu tujuan yang sama serta dapat bertukar data informasi dari komputer satu ke komputer yang lain yang saling terhubung.

Pengertian lain dari suatu jaringan komputer juga berhubungan langsung dengan penyampaian pesan yang bisa dilakukan melalui beberapa titik-titik atau nodes yang terhubung satu sama lain, berupa dengan kabel atau tanpa kabel (nirkabel). Jaringan ini biasa digunakan oleh komputer maupun telepon untuk menyampaikan pesan melalui beberapa sistem yang ada pada komputer atau telepon itu sendiri.

2.2 Virtual Local Area Network (VLAN)

2.2.1 Pengertian VLAN

VLAN merupakan suatu model jaringan yang tidak terbatas pada lokasi fisik seperti LAN, Hal ini mengakibatkan suatu network dapat dikonfigurasi secara virtual tanpa harus menuruti lokasi fisik peralatan. Penggunaan VLAN akan membuat pengaturan jaringan menjadi sangat fleksibel dan mudah untuk dipahami, dimana dapat dibuat segmen yang bergantung pada organisasi atau perusahaan, tanpa bergantung pada lokasi *workstation* atau tempat dimana VLAN tersebut dipasang.

Dari definisi di atas, dapat disimpulkan bahwa VLAN adalah sebuah teknologi pengembangan dari LAN yang berada pada jaringan layer 2 yang dapat membagi dari satu LAN menjadi beberapa LAN atau *broadcast domain*.

2.2.2 Manfaat VLAN

1. Meningkatkan *Performance*

Menurut (Asfihan, 2022) Dari segi kinerja, VLAN dapat menciptakan layer datar 2 jaringan menjadi sejumlah grup kerja logis guna meminimalisir beban *traffic* pada jaringan. Hal ini bertujuan untuk mengasingkan antara jaringan non esensial dan jaringan urgen sehingga performanya semakin optimal.

2. Mempermudah Administartor Jaringan

Manfaat VLAN berikutnya merupakan penyederhanaan proses administrasi. Setiap kali komputer berpindah tempat, maka komputer harus di konfigurasi ulang agar mampu berkomunikasi dengan jaringan dimana komputer itu berada. Dengan adanya jaringan VLAN suatu komputer server tidak butuh datang langsung ke lokasi komputer server guna untuk masuk ke jaringan. Semua komputer dapat terkoneksi dan mencapai server dari lokasi lain, adapun eksistensi komputer server mempermudah administrator untuk mengerjakan pengaturan dan kontrol terhadap jaringan supaya lebih aman.

3. Mengurangi Biaya Pemasangan

Dengan berpindahnya lokasi, maka akan menyebabkan biaya instalasi ulang. Dalam menggunakan jaringan VLAN, hal ini dapat di minimalisir.

4. Keamanan

VLAN dapat membatasi user yang bisa mengakses suatu data berdasarkan *access list* yang di tentukan, sehingga dapat meminimalisir penyalahgunaan hak akses.

2.2.3 Link VLAN

1. *Access Link*

Access Link merupakan tipe *link* yang umum dan dimiliki oleh hampir semua jenis *switch* VLAN. *Access Link* lazimnya digunakan untuk menghubungkan komputer dengan *switch*. *Access Link* tidak lain merupakan *port switch* yang sudah terkonfigurasi. *Access Link* mendukung teknologi *Ethernet* biasa (10 Mbps) hingga *FastEthernet* (100 Mbps).

Selama proses transfer data, *switch* akan membuang informasi tentang VLAN. Anggota suatu VLAN tidak dapat berkomunikasi dengan anggota VLAN lain, kecuali jika dihubungkan oleh *router*.

2. *Trunk Link*

Istilah *Trunk* diambil dari sistem telepon yang dapat mengangkut beberapa percakapan sekaligus. *Trunk Link* digunakan untuk menghubungkan *switch* dengan *switch* yang lain, *switch* dengan *router*, atau *switch* dengan server. Jadi, *port* telah dikonfigurasi untuk dilalui berbagai VLAN (tidak hanya sebuah VLAN).

Trunk Link hanya mendukung teknologi *Fast* (100 Mbps) atau Gigabit (1000 Mbps) *Ethernet*, sebab *Trunk Link* lazimnya dihubungkan dengan *network backbone* berkecepatan tinggi. Wajar jika kebutuhannya lebih tinggi dibanding *Access Link*.

Untuk memudahkan memahami kedua *link* tersebut, *Access Link* dianalogikan seperti jalan menuju pekarangan rumah, sedangkan *Trunk Link* seperti jalan umum. Lazimnya, jalan umum boleh dilalui oleh semua pengguna jalan, sedangkan jalan menuju pekarangan rumah hanya dilalui oleh pemilik rumah atau tamu yang ingin berkunjung ke rumah tersebut.

2.2.4 Tipe VLAN

1. Static VLAN

Static VLAN merupakan tipe VLAN yang umum dan paling *secure*. Setiap anggota dari suatu VLAN ditentukan berdasarkan nomor *port switch*. Kadangkala *static* VLAN disebut sebagai *port based* VLAN.

Pada *static* VLAN, proses konfigurasi relatif cukup mudah. Sebagai contoh, *port* 1 – 10 untuk VLAN 1 dan *port* 2 - 7 untuk VLAN 2.

2. Dinamis VLAN

Pada dinamis VLAN, keanggotaan akan ditentukan secara otomatis menggunakan *software* yang diinstal pada server pusat yang disebut VLAN *Management Policy Server* (VMPS). Contoh *software*-nya adalah CiscoWorks 2000. Dengan menggunakan VMPS, anggota VLAN dapat ditentukan berdasarkan MAC *address*, protokol, dan aplikasi untuk membentuk *dynamic* VLAN.

2.2.5 VLAN Trunking Protokol

VTP merupakan Protokol milik Cisco yang memungkinkan *switch-switch* pada Cisco (yang terhubung) saling bertukar informasi. VTP memudahkan proses konfigurasi secara otomatis antar sesama *switch*. Dengan VTP, maka dalam membuat suatu VLAN cukup dengan konfigurasi pada salah satu *switch*. (Sofana, 2010)

Penjelasan di atas serupa dengan penjelasan Jesin A. (2014) dalam buku *Packet Tracer Simulator*. Jesin A. menjelaskan bahwa VTP muncul karena banyaknya jumlah VLAN yang dibuat. Oleh karena itu, dengan adanya VLAN, pengguna tidak perlu

melakukan konfigurasi VLAN pada setiap *switch*.

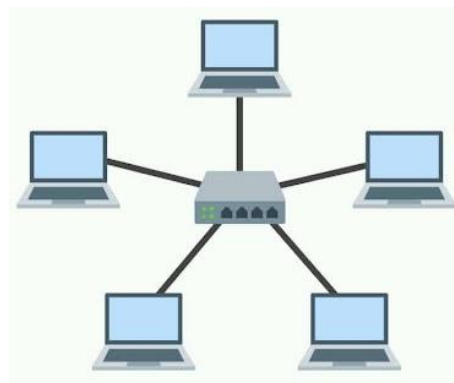
VTP dapat bekerja pada *layer 2*. Pengguna dapat menambah, menghapus mengedit dan mengubah konfigurasi VLAN. Jika salah satu *switch* dirubah konfigurasinya, maka VTP akan melakukan sinkronisasi konfigurasi terhadap *switch-switch* yang lain. (Sofana, 2010).

2.3 Topologi Jaringan

Topologi jaringan komputer merupakan suatu teknis, yang cara dan aturan di dalam membuat dan menghubungkan berbagai komputer dan perangkat terhubung lainnya ke dalam sebuah jaringan komputer. Topologi bersifat sebuah rancangan (desain), yang kemudian dapat diimplementasikan secara langsung melalui sejumlah perangkat keras penghubung pada jaringan komputer.

2.3.1 Topologi Star

Definisi Topologi *star* adalah menghubungkan semua perangkat komputer pada sentral atau pusat. Pusat yang dimaksud adalah sebuah *hub* atau *switch*. Topologi *star* umumnya digunakan pada jaringan komputer skala kecil dan menengah.



Gambar 2.1 Topologi Star

Topologi star memiliki sejumlah kelebihan. Adapun kelebihan-kelebihan topologi star tersebut antara lain mencakupi:

1. Topologi *star* lebih andal di dalam jaringan, di mana kemungkinan terjadinya tabrakan paket data (*collision*) kecil atau tidak ada sama sekali.
2. Topologi *star* mudah diimplementasikan, cukup dengan hanya menghubungkan komputer ke komputer server (termasuk juga pada *switch* atau *hub* jika dalam bentuk perangkat penghubung jaringan).
3. Kontrol terhadap akses pada topologi *star* lebih aman dan andal karena

terpusat kepada komputer *server* (atau dalam hal ini selain komputer juga dapat mencakup *hub* atau *switch* jika berupa perangkat penghubung).

4. Topologi *star* mendukung sifat *scalable* pada jaringan komputer, di mana penambahan maupun pengurangan jumlah komputer *client* yang terhubung, dapat dilakukan dengan mudah dan cepat sesuai dengan kebutuhan dan kondisi.
5. Topologi *star* relatif lebih fleksibel.
6. Topologi *star* mudah untuk diperbaiki dan dirawat (*maintenance*) termasuk juga jika ada kesalahan/gangguan.

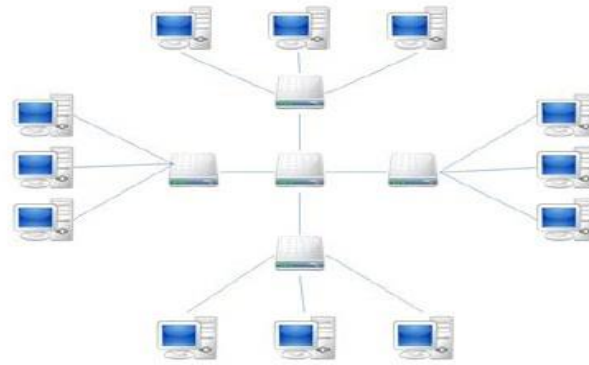
Tetapi topologi *star* juga memiliki sejumlah kekurangan. Kekurangan-kekurangan tersebut antara lain:

1. Karena sangat bergantung kepada komputer pusat atau *server* (maupun *hub* atau *switch* jika berupa perangkat penghubung), maka beban trafik dan kinerja dari komputer pusat (atau *hub* maupun *switch*) pada topologi *star* akan makin besar juga. Hal ini akan berisiko terhadap semakin cepatnya kerusakan pada perangkat keras dari sistem pada jaringan komputer.
2. Pada topologi *star* biaya jauh lebih besar, mengingat diperlukan kabel jaringan yang jauh lebih banyak.
3. Pada topologi *star*, apabila trafik jaringan padat (misalnya terdapat banyak pertukaran data antarkomputer), yang mana semua lalu lintas data melewati komputer pusat/*server* (maupun *hub* atau *switch*), akan berakibat pada lalu lintas pertukaran data yang makin melambat.

2.3.2 Topologi *Extended Star*

Topologi Jaringan *Extended Star* adalah sebuah topologi jaringan yang sama dengan topologi jaringan *star*, Akan tetapi pada Topologi Jaringan *Extended Star* memiliki lebih banyak *repeater* dalam satu mode pusat sehingga jangkauannya lebih panjang dibandingkan dengan topologi jaringan *star* biasa. (Abdi, 2018)

Topologi Jaringan *Extended Star* sendiri merupakan perkembangan dari topologi jaringan *star* dimana konsep dasar dari topologi jaringan ini adalah sama dengan topologi *star* hanya saja topologi ini memiliki jangkauan dan jumlah *host* lebih besar dibandingkan topologi *star* biasa. (Abdi, 2018)



Gambar 2.2 Topologi Extended Star

2.4 Perangkat Jaringan

2.4.1 Switch

Switch adalah komponen jaringan yang digunakan untuk menghubungkan beberapa *HUB* untuk membentuk jaringan yang lebih besar atau menghubungkan komputer - komputer yang mempunyai kebutuhan *bandwidth* yang besar. (Aditya, 2013)

Dari penjelasan di atas, maka dapat disimpulkan bahwa *switch* merupakan suatu *device* yang memiliki banyak *port* sehingga dapat menghubungkan lebih dari 2 komputer melalui *layer 2* atau *layer 3*. Oleh karena itu, *switch* disebut juga *multiport bridge* dan dapat menampung *bandwidth* dari yang terkecil yaitu 10Mb sampai terbesar yaitu 100Mb. *Switch* memiliki dua tipe yaitu *managed* dan *unmanaged*, *managed switch* adalah *switch* yang dapat dikonfigurasi port *access* dan port *trunkingnya*, serta dapat mengatur *bandwidth* pada masing-masing port yang ada di *managed switch*. Sedangkan *unmanaged switch* adalah *switch* yang tidak dapat dikonfigurasi port yang ada pada *switch*, sehingga *bandwidth* pada *unmanaged switch* aksesnya sama rata pada masing-masing port.



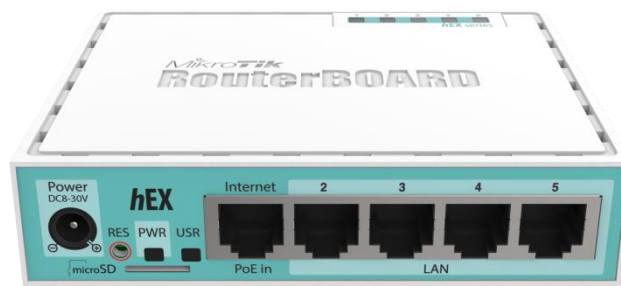
Gambar 2.3 Switch

2.4.2 Router Mikrotik

(Nadoel, 2011) *Mikrotik* RouterOS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi router *network* yang handal, mencakup berbagai fitur yang dibuat untuk *ip network* dan jaringan *wireless*.

Maka dapat disimpulkan definisi router adalah peralatan jaringan yang menghubungkan jaringan dengan jaringan yang lain. Sepintas router mirip dengan *bridge*, namun router lebih unggul dibandingkan *bridge*. Router bekerja menggunakan *routing* tabel yang disimpan di memori untuk membuat keputusan tujuan dan bagaimana paket dikirimkan. Router dapat memutuskan rute terbaik yang akan di tempuh oleh paket data (Irawan, 2013).

Router adalah salah satu komponen pada jaringan komputer yang mampu melewati data melalui sebuah jaringan atau internet menuju sasarannya, melalui sebuah proses yang dikenal sebagai routing (Rahmansyah, 2012). Router juga berfungsi untuk mengkoneksikan dua buah LAN (WAN dengan anggota dua LAN), LAN ke ISP (*Internet Service Provider*). Koneksi seperti ini menyebabkan semua *workstation* dapat terkoneksi ke internet selama 24 jam.



Gambar 2.4 Router Mikrotik

2.4.3 Access Point

Access Point adalah perangkat yang berfungsi sebagai *bridge* antara antenna jaringan nirkabel (*wireless*) dan jaringan kabel WLAN melalui konektor UTP RJ-45. Selain itu *access point* memiliki fungsi sebagai penghubung jaringan *wire* dengan jaringan *wireless*, serta pengganti media kabel dan sebagai solusi kepada pengguna yang memiliki mobilitas yang tinggi. Fungsi lain dari *access point* adalah mengubah sinyal radio

frequency menjadi sinyal digital yang akan disalurkan melalui kabel, atau disalurkan ke perangkat WLAN yang lain dan diubah ulang menjadi sinyal radio *frequency* yang dapat ditangkap oleh pengguna melalui perangkat pendukung seperti PC, mobile/handphone dan lain-lain.

Perangkat *access point* mempunyai peranan yang vital sebagai *interface* antara user dan jaringan *wireless* (nirkabel), pertukaran informasi antara perangkat *wireless* yang berbeda dan antara perangkat satu dengan perangkat lainnya. Sistem komunikasi nirkabel akan baik apabila perangkat seperti *access point* memiliki kinerja dan spesifikasi yang baik (Dr. Vladimir, 2019).



Gambar 2.5 Access Point

2.4.4 Access Point Controller

Access Point Controller adalah perangkat yang berfungsi mengolah dan mengkonfigurasi IP didalam *access point*. *Access point controller* yang dimaksud adalah *Omada Controller*. *Omada Controller* merupakan perangkat lunak manajemen untuk perangkat EAP TP-Link yang bersifat *cloud*. Dengan perangkat lunak ini, dapat menggunakan browser web untuk mengelola perangkat *Extensible Authentication Protocol* (EAP) secara terpusat, seperti mengkonfigurasi EAP dalam *batch* dan melakukan pemantauan EAP kapan saja. (Herfandi, 2021)



Gambar 2.6 Access Point Controller

2.5 Winbox

(Permatasari, 2015) *Winbox* adalah sebuah *utility* yang digunakan untuk melakukan *remote* ke *server Mikrotik* dalam mode GUI (*Graphical User Interface*). Jika untuk mengkonfigurasi *mikrotik* dalam teks mode melalui PC itu sendiri, maka untuk 13 mode GUI yang menggunakan *winbox* ini kita mengkonfigurasi *mikrotik* melalui komputer *client*. Mengkonfigurasi *mikrotik* melalui *winbox* lebih banyak digunakan karena selain penggunaanya yang mudah dan juga tidak harus menghafal perintah-perintah *console*. Fungsi utama *winbox* adalah untuk melakukan *setting* pada *mikrotik* router seperti manajemen *bandwidth*.

2.6 Cisco Packet Tracer

(Purnawan, 2018) Cisco *Packet Tracer* menurut para ahli yaitu: Menurut Dian Ariawal dan Onno W Purbo, (2016:3), Cisco *Packet Tracer* adalah *software* simulator yang di luncurkan oleh Cisco Sistem yang di fungsikan sebagai media pembelajaran, pelatihan, dan juga penelitian simulasi jaringan komputer. Menurut Iwan Sofana, (2015), Cisco *Packet Tracer* adalah *software* simulasi yang digunakan membuat jaringan komputer.

Dari penjelasan di atas, dapat disimpulkan bahwa Cisco *Packet Tracer* adalah *software* simulasi yang berfungsi sebagai tahap awal untuk membangun jaringan komputer. Dan juga untuk meneliti jalannya jaringan komputer tersebut.

2.7 TCP/IP

Menurut Nugroho (2013) “TCP/IP adalah sebuah perangkat lunak jaringan komputer yang terdapat dalam satu sistem dan memungkinkan komputer satu dengan

komputer lain dapat mentransfer data dalam satu grup network atau jaringan.

TCP singkatan dari *Transmission Control Protocol* dan IP singkatan dari *Internet Protocol*. TCP/IP menjadi satu nama karena fungsinya selalu bergandengan satu sama lain dalam komunikasi data. Adapun komponen didalam IP terbagi atas 2 bagian yaitu net ID dan Host ID. Net ID adalah bagian dari alamat yang mewakili jaringan fisik dari host sedangkan host ID adalah bagian yang mewakili bagian individu dari alamat. (Sujarweni, 2018)

Dari penjelasan diatas, dapat disimpulkan TCP/IP adalah perangkat lunak pada jaringan komputer yang berfungsi sebagai penghubung komputer satu dengan komputer lain dalam jaringan yang sama untuk mentransfer suatu data.

2.8 Subnetting

Subnetting merupakan proses pembagian atau pemecahan jaringan ke dalam beberapa sub jaringan dengan jumlah host yang lebih sedikit. (Soepomo, 2013) Tujuan dilakukanya subnetting diantaranya adalah sebagai berikut :

1. Mempermudah dalam mengontrol atau mengatur sebuah jaringan.
2. Efisiensi penggunaan ip address.s
3. Untuk menentukan batas network ID dalam suatu subnet.
4. Memperbanyak jumlah network (LAN).
5. Mengurangi jumlah host dalam suatu jaringan.
6. Untuk mengurangi tingkat kongesti (gangguan atau tabrakan) lalu lintas data dalam suatu jaringan.

Jaringan bisa dibagi menjadi beberapa jaringan kecil dengan membagi *IP* address dengan pembagiannya yang disebut sebagai subnetmask atau biasa juga disebut netmask. Netmask memiliki format sama seperti IP address. Di mana x adalah banyaknya binary 1 pada oktet terakhir subnetmask.

2.9 DHCP Server

DHCP (*Dynamic Host Configuration Protocol*) adalah protokol yang dipakai untuk memudahkan penyebaran alamat IP (*internet protocol*) secara otomatis ke perangkat lainnya. DHCP *server* adalah sebuah perangkat yang bertugas untuk mengatur dan memberikan alamat IP secara otomatis kepada komputer client yang ada. Sementara itu, komputer /perangkat lain seperti handphone yang menerima alamat IP dari DHCP server

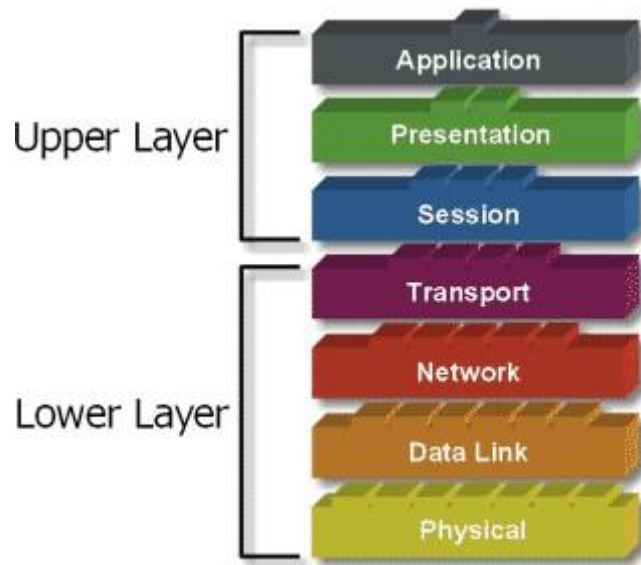
disebut **DHCP client**.

2.10 OSI Layer

Menurut Iwan Sofana (2010). OSI (*Open System Interconnetion*) layer merupakan salah satu arsitektur jaringan yang sering digunakan untuk menjelaskan bagaimana komputer jaringan bekerja secara logis. (Hamimah, 2011) Secara umum, model OSI membagi berbagai fungsi jaringan menjadi 7 lapisan. Itu lembaga yang menerbitkan model OSI adalah International Organization for Standardization (ISO). Ini model diperkenalkan pada tahun 1984. Lapisan OSI dibagi menjadi 7 bagian, yaitu:

1. *Application Layer*, *Application layer* merupakan lapisan ketujuh dan merupakan lapisan teratas dalam model OSI. Lapisan ini menyediakan antarmuka antara aplikasi yang digunakan untuk berkomunikasi dan jaringan yang mendasarinya melalui mana pesan kami ditransmisikan. Protokol lapisan aplikasi digunakan untuk bertukar data antara program yang berjalan pada host sumber dan tujuan.
2. *Presentation Layer*, Lapisan presentasi bertanggung jawab untuk menyajikan data ke lapisan aplikasi. Itu lapisan presentasi seperti penerjemah jaringan.
3. *Session Layer*, Lapisan sesi bertugas untuk menetapkan dan mengakhiri sesi (sesi) antara dua berkomunikasi host.
4. *Transport Layer*, Lapisan *transport* adalah lapisan yang tugasnya memastikan pesan yang dikirim bebas dari kesalahan.
5. *Network Layer*, Lapisan jaringan adalah lapisan ketiga dalam lapisan OSI. Layanan jaringan menyediakan layanan untuk pertukaran satu bagian data melalui jaringan antara perangkat perangkat akhir.
6. *Data Link Layer*, Lapisan data link menyediakan sarana untuk bertukar data melalui media lokal umum.
7. *Physical Layer* Lapisan fisik adalah lapisan OSI yang terletak di bagian bawah. Lapisan fisik mendefinisikan media transmisi jaringan ke media fisik dan membawa sinyal ke lapisan yang lebih tinggi.

Model Layer OSI dibagi dalam dua group: *upper layers* dan *lower layers*. *Upper layers* fokus pada aplikasi pengguna dan bagaimana file direpresentasikan di komputer. Untuk *Network Engineer*, bagian utama yang menjadi perhatiannya adalah pada *lower layers*. *Lower layer* adalah intisari komunikasi data melalui jaringan aktual.



Gambar 2.7 OSI Layer

Beberapa keuntungan atau alasan mengapa model OSI dibuat berlapis-lapis, diantaranya: (Sofana, 2010)

1. Memudahkan siapa saja (khususnya pemula) untuk memahami cara kerja jaringan komputer secara menyeluruh.
2. Memecah persoalan komunikasi data yang rumit menjadi bagian-bagian kecil yang lebih sederhana, sehingga dapat memudahkan proses *trouble shooting*.
3. Memungkinkan *vendor* atau pakar *network* mendesain dan mengembangkan *hardware/software* yang sesuai dengan fungsi *layer* tertentu (modular).
4. Menyediakan standar *interface* bagi pengembangan perangkat yang melibatkan *multivendor*. Adanya abstraksi *layer* memudahkan pengembangan teknologi masa depan yang terkait dengan *layer* tertentu.

Berikut ini adalah tabel untuk menjelaskan fungsi setiap *layer* beserta contoh-contoh protokol yang sesuai untuk masing-masing *layer* :

Tabel 2.1 OSI Layer

Layer	Fungsi	Contoh Protokol
<i>Application</i>	Menyediakan servis bagi aplikasi <i>Network</i>	NNTP, H7, Modbus, SIP, SSI, DHCP, FTP, Gopher, HTTP, NFS, NTP, RTP, SMPP, SMTP, SNMP, Telnet
<i>Presentation</i>	Mengatur konversi dan translasi berbagai format data, seperti kompresi data dan enkripsi data	TDI, ASCII, EBCDIC, MIDI, MPEG, ASCII7
<i>Session</i>	Mengatur sesi (<i>session</i>) yang meliputi <i>establishing</i> (memulai sesi), <i>maintaining</i> (mempertahankan sesi), dan <i>terminating</i> (mengakhiri sesi) antar entitas yang dimiliki oleh <i>presentation layer</i>	SQL, X Window, Named Pipes (DNS), NetBIOS, ASP, SCP, OS Scheduling, RPC, NFS, ZIP
<i>Transport</i>	Menyediakan <i>end-to-end communication protocol</i> . Layer ini bertanggung jawab terhadap “keselamatan data” dan “segmentasi data”, seperti: mengatur <i>flow control</i> (kendali aliran data), <i>error detection</i> (deteksi error) and <i>correction</i> (koreksi), <i>data sequencing</i> (urutan data) dan <i>size of the packet</i> (ukuran paket)	TCP, SPX, UDP, SCTP, IPX

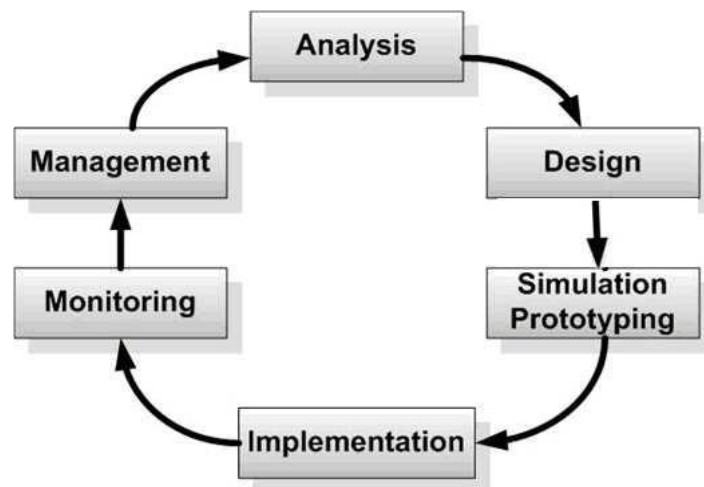
<i>Network</i>	Menentukan rute yang dilalui oleh data. <i>Layer</i> ini menyediakan <i>logical addressing</i> (pengalamatan logika)	IPX, IP, ICMP, IPSec, ARP, RIP, IGRP, BGP, OSPF, NBF, Q.931
----------------	--	---

2.11 Metode NDLC (*Network Development Life Cycle*)

Network Development Life Cycle (NDLC) merupakan suatu metode yang digunakan dalam mengembangkan atau merancang jaringan infrastruktur yang memungkinkan terjadinya pemantauan jaringan untuk mengetahui statistik dan kinerja jaringan. Hasil analisis kinerja tersebut dijadikan sebagai pertimbangan dalam perancangan desain jaringan, baik desain jaringan yang bersifat fisik atau jaringan logis. NDLC terdiri dari enam tahapan, yaitu *analysis*, *design*, *simulation prototyping*, *implementation*, *monitoring* dan *management*. (Aziz, 2017)

Pada penelitian ini menggunakan 3 tahapan pada metodologi NDLC, yaitu:

1. *Analysis*
2. *Design*
3. *Simulation prototyping*



Gambar 2.8 Tahapan NDLC

Adapun penjelasan dari tahapan NDLC sebagai berikut yaitu (Puspita et al., 2015) :

2.11.1 *Analysis*

Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan user, dan analisa topologi atau jaringan yang sudah ada saat ini.

2.11.2 Design

Tahap desain ini akan membuat gambar desain topologi jaringan yang akan dibangun. Desain bisa berupa *design structure topology*, *design access data*, desain tata layout perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang proyek yang akan dibangun. Hasil dari design berupa:

1. Gambar-gambar topology (*server farm*, *firewall*, *datacenter*, *storages*, *lastmiles*, perkabelan, titik akses dan sebagainya).
2. Gambar-gambar *detailed* estimasi kebutuhan yang ada.

2.11.3 Simulation

Pada tahap ini beberapa *network engineer* akan membuat dalam bentuk simulasi dengan bantuan *tools* khusus di bidang *network* seperti BOSON, Packet Tracer, NETSIM, dan sebagainya, hal ini dimaksudkan untuk melihat kinerja awal dari network yang akan dibangun.

2.11.4 Implementation

Dalam tahap implementasi *network engineer* akan menerapkan semua yang telah direncanakan dan di desain sebelumnya.

2.11.5 Monitoring

Tahapan *monitoring* merupakan tahapan yang penting agar jaringan dapat berjalan sesuai dengan keinginan dan tujuan dari user pada tahap awal analisis

2.11.6 Management

Pada tahap ini suatu kebijakan perlu dibuat untuk membuat atau mengatur agar sistem yang telah dibangun dapat berjalan dengan baik dan dapat berlangsung lama.