BAB II
LANDASAN TEORI

2.1. Kajian Pustaka

Ada beberapa penelitian yang dilakukan tentang analisis desain jaringan komputer menggunakan metode *Top-down* antara lain penelitian yang menjelaskan keefektifan metode *Top-down* adalah penelitian dari Muhammad Nur Ikhsanto dan Handoyo Widi Nugroho yang berjudul "Analisis Performa dan Desain Jaringan Komputer Menggunakan *Top-down Network* Desain Studi Kasus pada CV. Merah Putih" penelitian tersebut menjabarkan "Analisis kebutuhan pada *Top-down Network disain* terdiri dari analisis bisnis, analisis teknis, analisis karakteristik jaringan dan analisis lalu lintas jaringan. *Logical network* meliputi perencanaan desain *topologi* jaringan, perencanaan *IP addrees*, perencanaan *switching* dan *routing*, dan perencanaan manajemen jaringan. Desain fisik meliputi analisa pemilihan teknologi dan peralatan yang digunakan dalam jaringan (Ikhsanto dan Nugroho, 2015).

Penelitian dari Maria Ulfa berjudul "*Top Down Network Design* dalam Perancangan Jaringan Komputer pada SMA Negeri 1 Indralaya Selatan" . Penelitian ini membuktikan metode *Top-down* memberikan gambaran yang lebih jelas tentang perencanaan jaringan komputer Penelitian ini menghasilkan desain *topologi* baru dan desain manajemen tata letak komponen jaringan dimana disesuaikan dengan kebutuhan agar memaksimalkan semua aktivitas dan proses pembelajaran yang menggunakan layanan *internet* dan *intranet* pada jaringan *LAN* dan *WLAN* SMA Negeri 1 Indralaya Selatan. Penambahan infrastruktur seperti perangkat *mikrotik router board* dan komputer *server* sebagai *server database* maka akan semakin mudah untuk memanajemen jaringan komputer seperti manajemen pengguna (*user*), manajemen *bandwidth upload* dan *download* pada setiap bagian ruang seperti kantor, guru, laboratorium dan perpustakaan (Ulfa, 2017).

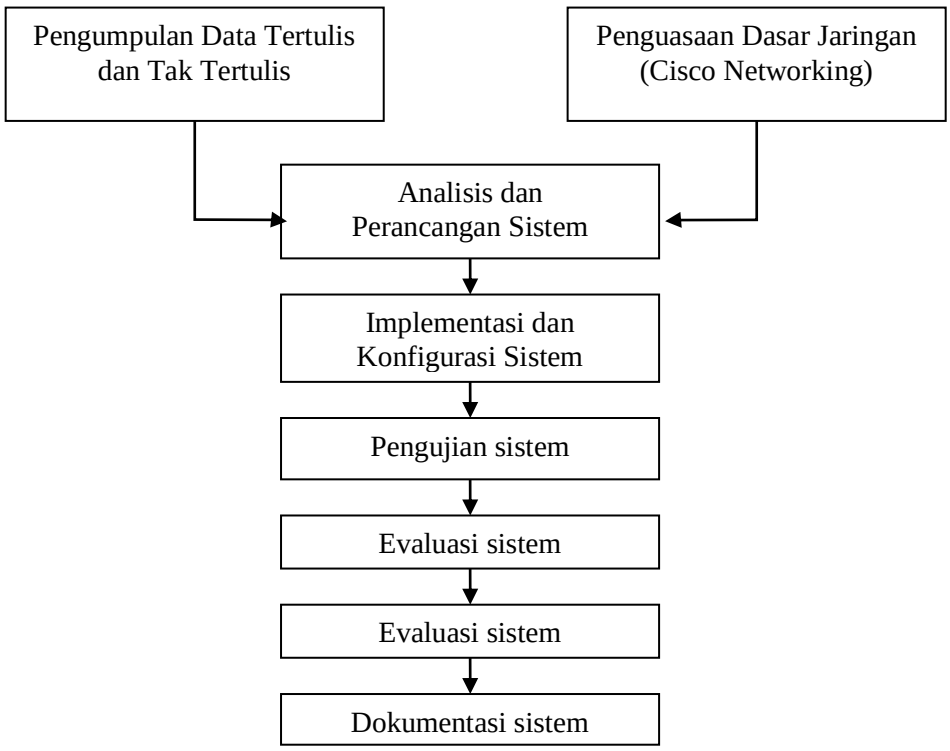
Hasil penelitian tersebut dikuatkan oleh peneliti Syahril Rizal dan Benny Wilson Saputra yang berjudul "Penerapan Metode *Top-down* dalam Pengembangan Jaringan

Komputer Lokal Perusahaan". Penelitian tersebut menjelaskan "*Top-Down Approach* merupakan suatu pendekatan pengembangan sistem jaringan komputer yang bisa diterapkan karena berorientasi kepada area bisnis, karena komponen puncak akan menyediakan semua kebutuhan yang diperlukan agar tercapainya target bisnis" (Rizal dan Saputra, 2018).

Menurut penelitian dari Amri Eka Widayanto, Dahlan Susilo dan Firdhaus Hari Saputro Al Haris yang berjudul "Manajemen *Bandwidth* dengan *Simple Queue* dan *Queue Tree* di Laboratorium Komputer Universitas Sahid Surakarta". Penelitian tersebut menjelaskan "Berdasarkan nilai QoS versi TIPHON menunjukkan bahwa pengujian sistem antrian *Simple Queue* dan *Queue Tree* ketika *upload* data menghasilkan nilai memuaskan dengan indeks 3,5" (Widayanto, dkk, 2016)

2.2. Kerangka Pemikiran

Berdasarkan permasalahan yang terkait akan dibuat sebuah kerangka berpikir yang nantinya dapat mempermudah dalam melakukan penelitian. Untuk gambar kerangka berpikir yang sudah dibuat dapat dilihat pada Gambar 2.1



Gambar 2. 1. Kerangka Pemikiran

2.3. Desain dan Konfigurasi

Menurut Pakpahan (2015), desain jaringan komputer adalah melakukan perancangan dan menganalisis sistem jaringan yang akan dibangun yang meliputi seluruh aspeknya mulai dari komponen *hardware* dan *software*, layanan dan sebagainya. Kemudian menentukan rancangan konfigurasi yaitu skema pengalamatan, topologi yang digunakan dan pelayanan yang akan diberikan oleh jaringan tersebut serta pengelolaannya

2.4. Jaringan Komputer

Sistem jaringan komputer merupakan sebuah sistem yang terdiri atas komputer dan perangkat jaringan lainnya yang bekerja sama untuk mencapai suatu tujuan yang sama antara lain : membagi sumber daya dan mudah dalam berkomunikasi antar komputer (Madcom, 2015).

2.4.1. Jaringan Komputer Berdasarkan Ukuran

Menurut Prakasa (2019), Secara umum, jaringan komputer dapat dibedakan berdasarkan luasan area-nya. Jaringan komputer dibedakan menjadi empat tipe yaitu :

a. Personal Area Network / Body Area Network

Personal Area Network disebut juga dengan *Body Area Network* adalah jaringan komputer dengan cakupan luas area seukuran tubuh manusia atau di sekitar tubuh manusia. Jaringan komputer ini biasanya digunakan untuk perangkat *Wireless* seperti *Wireless headphone*, *Wireless mouse*, *Wireless microphone* dan lain sebagainya seperti pada Gambar 2.2 .

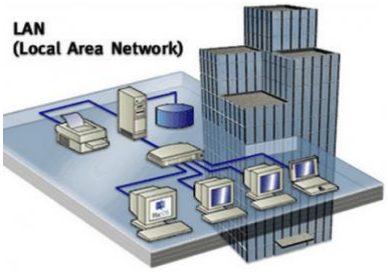
Sumber : Prakasa (2019)

Gambar 2. 2. Ilustrasi *Personal Area Network*

b. Local Area Network

Local Area Network merupakan jaringan komputer dengan luasan area lokal yang terbatas seperti pada area perkantoran, perumahan atau sekolah. Sampai saat ini masih belum terdapat literatur yang menyebutkan batasan khusus luas area *Local Area Network* namun yang dapat dijadikan panduan adalah selama jaringan komputer tersebut beradapada 1 area yang sama dari sebuah institusi (perusahaan / sekolah / gedung dll). Beberapaliteratur menyebutkan bahwa luasan maksimal yang disarankan untuk membangun *Local Area Network* kurang dari 1 km.

Tujuan dari dibangunnya *Local Area Network* adalah untuk berbagi sumber daya (*printer*, *file*, koneksi *internet* dll). Sehingga perusahaan tidak perlu berinvestasi perangkat terlalu banyak (*printer*, *scanner* dll). Pada kondisi saat ini *Local Area Network* dilengkapi dengan jaringan nirkabel (*Wireless LAN*) untuk memudahkan staf yang menggunakan perangkat bergerak (laptop / *smart devices*). Ilustrasi *Local Area Network* dapat dilihat pada Gambar 2.3 .

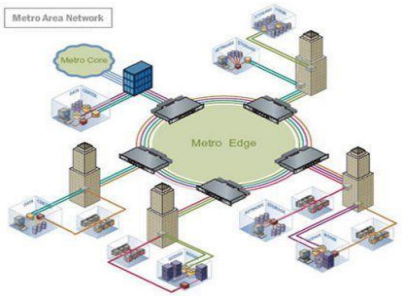


Sumber : Prakasa(2019)

Gambar 2. 3. Ilustrasi *Local Area Network*

c. Metropolitan Area Network

Seperti namanya, *Metropolitan Area Network* menghubungkan jaringan komputer pada luasan area seukuran kota. *Metropolitan Area Network* akan menghubungkan antar *Local Area Network* yang ada pada beberapa kantor / lokasi yang berjauhan namun masih dalam lingkup 1 kota sehingga staf dapat berbagi sumber daya dengan staf lain di kantor / lokasi yang lain. Biasanya digunakan pada perusahaan yang memiliki cabang di beberapa lokasi namun masih dalam wilayah 1 kota. Ilustrasi *Metropolitan Area Network* dapat dilihat pada Gambar 2.4 .

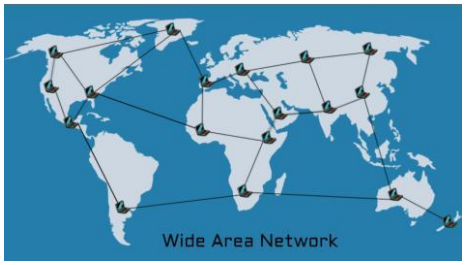


Sumber : Prakasa(2019)

Gambar 2. 4. Ilustrasi *Metropolitan Area Network*

d. Wide Area Network

Wide Area Network merupakan jaringan komputer terbesar yang menghubungkan banyak *Metropolitan Area Network* . Konsep awal dari *Wide Area Network* adalah untuk menghubungkan beberapa kantor cabang perusahaan multinasional yang ada di beberapa negara yang berbeda sehingga meskipun berada pada lokasi yang berjauhan tetap dapat terhubung dalam 1 jaringan komputer. Ilustrasi *Wide Area Network* dapat dilihat pada Gambar 2.5



Sumber : Prakasa(2019)

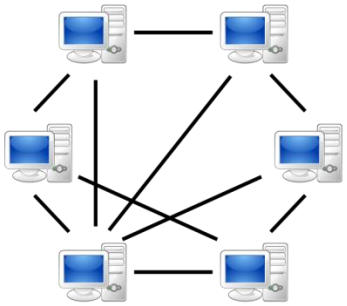
Gambar 2. 5. Ilustrasi *Wide Area Network*

2.4.2. Model Jaringan

Menurut Madcom (2015), terdapat dua model jaringan yang dapat digunakan dalam sistem jaringan komputer yaitu: model jaringan *Peer to Peer* (P2P) serta model jaringan *Client-Server*.

a. Peer to Peer

Model jaringan *Peer to Peer* (P2P) memungkinkan seorang *user* untuk membagi sumber daya yang ada pada komputernya, baik itu berupa data/informasi, *hardware*, dan lain-lain serta mengakses sumber daya yang terdapat pada komputer lain. Ilustrasi *Peer to Peer* dapat dilihat pada Gambar 2.6 .

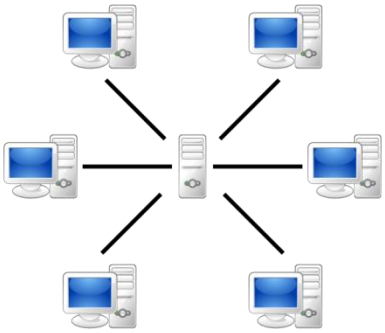


Sumber : https://en.wikipedia.org/wiki/Peer-to-peer

Gambar 2. 6. Ilustrasi *Peer to Peer*

b. Client-Server

Model jaringan komputer *Client-Server* memungkinkan untuk mensentralisasikan fungsi dan aplikasi kepada satu atau dua komputer sebagai sebuah *server* menjadi jantung dari keseluruhan sistem, memungkinkan mengakses sumber daya dan menyediakan keamanan bagi *client* selama masih terhubung dalam suatu jaringan komputer. Ilustrasi *Client-Server* dapat dilihat pada Gambar 2.7 .



Sumber : https://en.wikipedia.org/wiki/Peer-to-peer

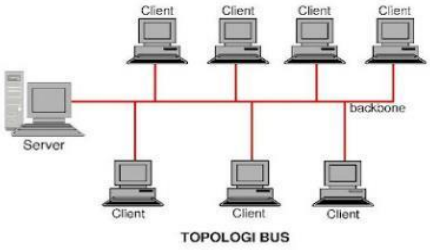
Gambar 2. 7. Ilustrasi *Client-Server*

2.4.3. *Topologi* Jaringan Komputer

Menurut Prakasa (2019), topologi jaringan komputer merupakan bentuk dari jaringan komputer yang dibuat. Pemahaman tentang bentuk jaringan komputer sangat penting untuk dikuasai sehingga jaringan komputer yang didesain dan dikelola dapat berjalan dengan optimal. *Topologi* jaringan komputer terus berkembang seiring perkembangan kebutuhan akan jaringan komputer, sehingga masing-masing *topologi* jaringan komputer memiliki kelebihan dan kekurangannya. *Topologi* jaringan komputer dibedakan menjadi lima tipe yaitu :

a. *Topologi BUS*

Topologi BUS merupakan *topologi* jaringan komputer yang pertama kali dikembangkan. *Topologi* ini secara sederhana menyambungkan beberapa komputer secara pararel seperti pada Gambar 2.8 di bawah ini. Ciri khas dari topologi ini adalah adanya *backbone* yang menghubungkan setiap perangkat komputer.

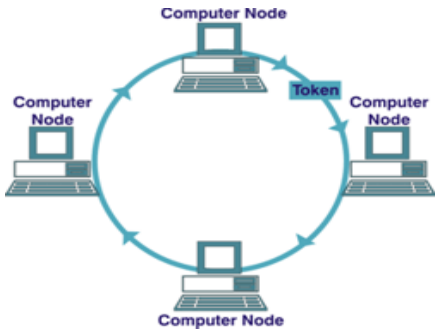


Sumber : Prakasa(2019)

Gambar 2. 8. Ilustrasi *Topologi BUS*

b. Topologi Ring

Pada dasarnya *topologi Ring* merupakan *topologi Bus* yang kedua ujungnya disambungkan seperti pada Gambar 2.9 di bawah ini. *Topologi Ring* berusaha untuk memecahkan permasalahan *data collision* yang terjadi pada *topologi Bus* dengan menggunakan *Token*. *Token* merupakan sebuah data khusus yang berputar secara terus menerus di dalam jaringan *Ring*. Hanya Komputer yang mendapatkan *Token* yang dapat mengirimkan data (*transmit*) sedangkan komputer lainnya dalam keadaan *receive* (menerima data). Dengan teknik ini *data collision* dapat diminimalisir karena pada suatu waktu hanya ada 1 komputer yang mengirimkan datanya (yang lain pada *mode receive*).

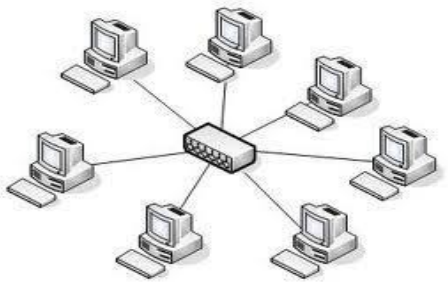


Sumber : Prakasa(2019)

Gambar 2. 9. Ilustrasi *Topologi Ring*

c. *Topologi Star*

Topologi Star merupakan *topologi* yang berlawanan dengan konsep *topologi Ring* bahwa jaringan komputer sebaiknya dibuat secara terdistribusi dan tidak saling terkait. Dengan demikian maka apabila terdapat permasalahan pada sebuah komputer tidak mempengaruhi komputer lainnya. Namun *topologi* ini membutuhkan perangkat sebagai pusat jaringan komputer yang disebut dengan *konsentrator* seperti pada Gambar 2.10 . Pada implementasinya *konsentrator* dapat berupa *Hub / Switch*.

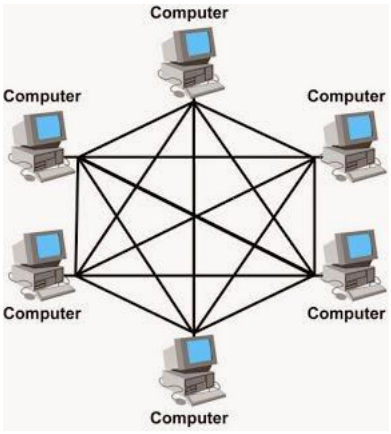


Sumber : Prakasa(2019)

Gambar 2. 10. Ilustrasi *Topologi Star*

d. *Topologi mesh*

Topologi mesh berusaha untuk menyelesaikan permasalahan pada *topologi Star* yaitu menghilangkan *konsentrator* pada jaringan komputer. Setiap komputer didesain untuk dapat terhubung ke komputer lain secara langsung (*peer to peer*) sehingga tidak membutuhkan adanya *konsentrator* seperti pada Gambar 2.11 berikut ini :

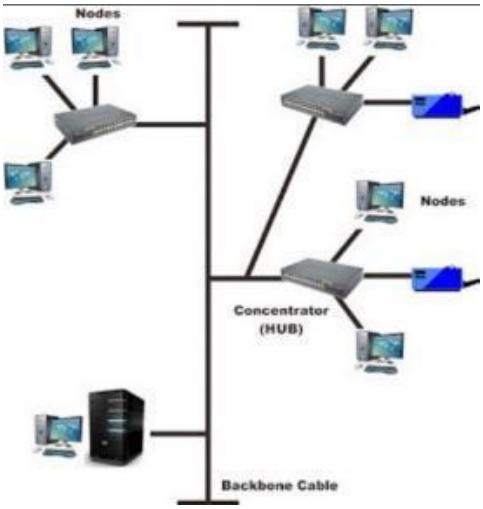


Sumber : Prakasa(2019)

Gambar 2. 11. Ilustrasi *Topologi Mesh*

e. Topologi Tree

Topologi Tree merupakan gabungan dari *topologi Bus & Star* dimana terdapat *backbone* yang menghubungkan banyak *topologi* Star seperti pada Gambar 2.12 berikut ini. *Topologi Tree* menggabungkan kecepatan *topologi Bus* dengan fleksibilitas *topologi Star*. Sehingga akan didapatkan jaringan komputer yang cepat namun tetap dapat berkembang secara fleksibel sesuai dengan kebutuhan.



Sumber : Prakasa(2019)

Gambar 2. 12. Ilustrasi *Topologi Tree*

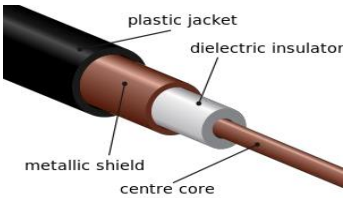
2.4.4. Media Transmisi

Menurut Prakasa (2019), perkembangan jaringan komputer tidak terlepas dari perkembangan media transmisi yang digunakan. Secara umum media transmisi yang digunakan untuk pengiriman data dibagi menjadi 2 kelompok besar yaitu *guided* & *unguided media*. *Guided media* merupakan media transmisi yang memiliki fisik yang dapat dilalui oleh data. Sedangkan *unguided media* adalah media transmisi yang tidak memiliki fisik sehingga data dapat terkirim ke semua arah (*broadcast*). Adapun media transmisi antara lain :

a. Coaxial

Coaxial merupakan salah satu media transmisi yang cukup populer karena telah tersedia secara umum di masyarakat. Kabel *coaxial* biasanya digunakan untuk kabel antena televisi. Karena ketersediaannya maka jaringan komputer pertama yang dikembangkan menggunakan media transmisi *coaxial*. Kabel

coaxial dapat di lihat pada Gambar 2.13 di bawah ini

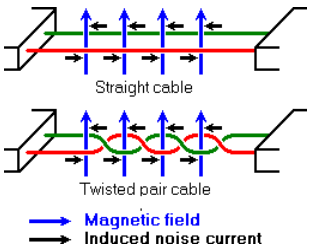


Sumber : Prakasa(2019)

Gambar 2. 13. Kabel *Coaxial*

b. Twisted Pair

Twisted Pair merupakan media transmisi yang umum digunakan pada jaringan komputer. Pada dasarnya *twisted pair* merupakan kabel tembaga yang dipilin. Tujuan dari pemilinan kabel ini adalah untuk mengurangi *noise* yang disebabkan oleh induksi magnetik sepert pada Gambar 2.14 berikut ini :



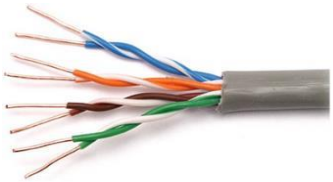
Sumber : Prakasa(2019)

Gambar 2. 14. *Twisting cable*

Sebagai media transmisi data, terdapat beberapa jenis kabel *twisted pair* sebagai berikut :

1) *Unshielded Twisted Pair* (*UTP*)

UTP merupakan kabel yang paling dikenal sebagai media transmisi di jaringan komputer. Selain harganya yang relatif murah, hampir seluruh perangkat jaringan komputer mendukung media transmisi jenis ini. Secara fisik kabel *UTP* dapat dilihat pada Gambar 2.15 berikut ini :



Sumber : Prakasa(2019)

Gambar 2. 15. Kabel UTP

2) *Shielded Twisted Pair* (*STP*)

Kabel *STP* pada dasarnya merupakan kabel UTP yang diberikan *shield* didalam pembungkusnya. *Shield* ini terbuat dari *aluminium foil* yang bertujuan untuk mengurangi interferensi magnetik dari sekitar kabel. Biasanya digunakan pada lokasi yang memiliki benda – benda yang mengeluarkan radiasi elektromagnetik. Secara fisik kabel STP dapat dilihat pada Gambar 2.16 berikut ini :

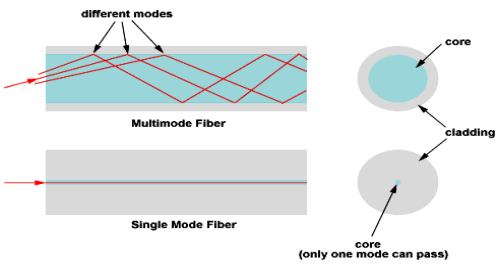
Sumber : Prakasa (2019)

Gambar 2. 16. Kabel STP

c. Fiber optic

Fiber optic merupakan salah satu terobosan baru di bidang media transmisi. Merupakan penyempurnaan dari teknologi sebelumnya yang dikenal dengan *infra red*. Kelebihan menggunakan *fiber optic* selain dapat mentransmisikan data dengan lebih cepat, pada *fiber optic* redaman hampir tidak ada sehingga sangat cocok untuk mentransmisikan data pada jarak yang jauh. Secara umum *fiber optic* dibagi menjadi 2 bagian yaitu *single-mode* dan *multi-mode* dapat dilihat pada Gambar 2.17 di bawah ini

Secara fisik, *Fiber Optic Single Mode* berukuran relatif kecil apabila dibandingkan dengan *Fiber Optic Multi Mode*. Pada *single mode* sebuah *fiber optic* hanya dapat mentransmisikan sebuah data dan sebaliknya pada *multi mode* dapat mentransmisikan banyak data secara bersamaan.



Sumber : Prakasa(2019)

Gambar 2. 17. *Multimode vs Singlemode Fiber Optic*

d. Wireless Radio

Transmisi data menggunakan jaringan komputer sendiri telah dilakukan mulai tahun 1970 yaitu ketika dikembangkannya jaringan komputer oleh University of Hawaii pada tahun 1971 menggunakan *Ultra High Frequency*. Penelitian tentang transmisi data nirkabel dilakukan oleh IEEE (*Institute Of Electrical & Electronics Engineers*) yaitu sebuah lembaga nirlaba yang bergerak di bidang pengembangan standar perangkat elektronik dan kelistrikan. Untuk jaringan nirkabel dikembangkan di bawah kelompok dengan kode 802.11. Perkembangan teknologi jaringan nirkabel disajikan pada Tabel 2.1.

Tabel 2. 1. *802.11 Protocols*

Tahun	Protokol Standard	Frekuensi	Max. Data rate
1997	802.11	2,4 Ghz	2 Mbps
1999	802.11a	5 Ghz	54 Mbps
1999	802.11b	2,4 Ghz	11 Mbps
2003	802.11g	2,4 Ghz	54 Mbps
2009	802.11n	2,4 / 5 Ghz	600 Mbps
2013	802.11ac	5 Ghz	1 Gbps
2013	802.11ad	60 Ghz	7 Gbps

2.4.5. *Hardware* Jaringan

Menurut Madcom (2015), dalam membangun sistem jaringan komputer khususnya jaringan kabel, diperlukan beberapa perangkat keras yang dapat disesuaikan sesuai kebutuhan. Adapun perangkat keras jaringan yaitu :

a. *LAN Card / Ethernet Card* (Kartu Jaringan)

Ethernet Card merupakan *hardware* jaringan yang dipasang pada sebuah PC yang berfungsi untuk dapat berkomunikasi dengan komputer lain melalui jaringan *LAN* (*Local Area Network*). *Ethernet Card* menggunakan kabel *coaxial, twisted pair*, dan dapat digunakan juga dalam *Wireless LAN* (W*LAN*). Setiap *Ethernet Card* memiliki *MAC Address* (*Medium Access Control*) yang unik dan berbeda-beda, hal tersebut berarti tidak ada dua buah *Ethernet Card* yang memiliki *MAC Address* yang sama.

b. *HUB*

HUB atau konsentrator adalah sebuah perangkat keras jaringan yang berfungsi menyatukan kabel-kabel jaringan. Selain itu *HUB* juga berfungsi sebagai penerima sinyal dari sebuah komputer, kemudian mentransmisikan ke komputer lain pada sebuah jaringan. Dengan kata lain *HUB* bekerja sebagai penyambung, *consentrator*, dan sebagai penguat sinyal pada kabel jaringan.

c. *Switch*

Switch hampir sama dengan *HUB* karena juga mampu menganalisis alamat tujuan dari data yang dikirim, namun memiliki *port* yang lebih banyak dan mampu untuk membangun sebuah jaringan. Pengalamatan yang dilakukan *switch* yaitu berdasarkan alamat fisik atau *MAC address* dari setiap perngkat yang terhubung ke *switc*h. Selain itu *switch* mampu melakukan penyaringan data yang lewat untuk dicek apakah ada yang rusak atau tidak.

d. *Modem*

Modem berasal dari singkatan dari *modulator de-modulator* merupakan perangkat yang digunakan untuk merubah sinyal analog menjadi sinyal digital dan sebaliknya dari sinyal digital menjadi sinyal analog. *Modem* digunakan untuk menghubungkan komputer dengan internet. *Modem* juga dapat digunakan untuk menghubungkan dua buah komputer dengan menggunakan *line* telepon.

e. *Repeater*

Repeater merupakan perangkat yang digunakan untuk menguatkan sinyal. *Reapeater* digunakan apabila menghubungkan perngkat dengan jarak yang berjauhan. *Reapeater* tidak hanya diperuntukan bagi jaringan kabel saja, namun sudah mendukung pada jaringan *Wireless* .

f. *Router*

Router adalah sebuah perangkat keras jaringan komputer yang mengirimkan paket data melalui sebuah jaringan atau *internet* menuju tujuannya melalui sebuah proses yang dikenal sebagai *routing* untuk menyambungkan jaringan *LAN* atau *WAN* ke jaringan *WAN* (*Internet*) atau menyambungkan dua atau lebih jaringan yang berbeda kelas. *Router* bekerja dengan melihat alamat asal

dan alamat tujuan dari paket data yang melewatinya dan memutuskan rute yang akan dilewati paket data tersebut untuk sampai ke tujuan. *Router* mengetahui alamat masing-masing komputer di lingkungan jaringan lokasi maupun *router* lainnya.

g. Bridge

Bridge merupakan perangkat keras jaringan untuk menghubungkan dua buah jaringan secara fisik yang menggunakan protokol sama/sejenis. *Bridge* juga bertugas mengirimkan paket-paket data, sehingga *bridge* memiliki kemampuan yang lebih baik dibandingkan dengan *HUB* atau *switch* karena *bridge* mampu membagi-bagi arus paket data ke segmen-segmen tertentu dengan sistem *filtering traffic*. Selain itu, *bride* juga dapat dikatakan sebagai media *expander* untuk menambah jangkauan dari sebuah jaringan *LAN* dan menghubungkannya dengan jaringan lainnya pada lokasi yang berbeda.

h. Fiber Optic Media Converter Box

Fiber Optic Media Converter Box adalah perangkat keras jaringan yang dapat menghubungkan dua jenis jaringan yang berbeda media penghantar seperti *twisted pair* dengan kabel *fiber optic*. *Media Converter Box Fiber Optic* mengubah sinyal elektrik ke sinyal optik atau sebaliknya.

i. Optical Termination Box (OTB)

Optical Termination Box (OTB) adalah tempat yang didesain khusus untuk menempatkan hasil terminasi / *splicing*.

j. Optical Distribution Point (ODP)

Optical Distribution Point (ODP) adalah tempat instalasi sambungan jaringan optik *single-mode* terutama untuk menghubungkan kabel *fiber optic* distribusi dan kabel *drop*

2.5. Open System Interconnection

Menurut Prakasa (2019), pada awal pengembangan jaringan komputer, perusahaan-perusahaan pembuat perangkat jaringan komputer membuat standar mereka sendiri. Sehingga antar perangkat jaringan komputer yang berbeda *merk* tidak dapat saling berkomunikasi. Untuk mengatasi hal ini maka beberapa

organisasi di bidang komputer bekerjasama untuk membuat sebuah standar untuk komunikasi data jaringan komputer. Hasil dari kerjasama ini kemudian dikenal dengan *Open System Interconnection (OSI)* yang terdiri dari 7 lapisan / layer. Setelah dihasilkannya *OSI*, maka setiap perusahaan pembuat perangkat jaringan komputer harus mendesain perangkatnya sesuai dengan *OSI* sehingga meskipun berbeda *merk*, perangkat jaringan komputer yang terstandar akan dapat saling berkomunikasi.

2.5.1. *Open System Interconnection Layers*

Menurut Prakasa (2019),OSI Layer, dapat dijelaskan sebagai berikut :

a. Layer 7 – Application Layer

Pada lapisan *Application* memberikan landasan kepada *software* yang akan menggunakan jaringan komputer seperti *web browser, email client, ftp client* dan lain sebagainya

b. Layer 6 – Presentation Layer

Lapisan di bawah *Application* adalah *Presentation.* Lapisan ini menerima data dari lapisan *Application* untuk kemudian di proses terlebih dahulu sebelum diteruskan kelapisan *session.* Salah satu proses yang cukup vital di lapisan ini adalah pemampatan /*compress* data. Tujuan dari pemampatan data adalah agar data yang dikirimkan dapat berukuran sekecil mungkin. Pada perangkat komputer penerima, data akan di *extractter* lebih dahulu sebelum diteruskan ke lapisan *Application.*

c. *Layer 5 – Session Layer*

Seperti pada namanya, lapisan *Session* berurusan dengan hubungan antara komputer pengirim dan penerima. Pada lapisan inilah dipastikan setiap pengguna akan mendapatkan informasi yang dimintanya meskipun banyak pengguna mengakses *server*secara bersamaan. Setiap pengguna akan mendapatkan identitas khusus sehingga tidak terjadi kekeliruan pengiriman data.

d. Layer 4 – Transport Layer

Lapisan *Transport* memegang peranan yang cukup penting pada komunikasi data. Pada lapisan ini dilakukan proses segmentasi paket. Segmentasi adalah proses pemecahan paket data sesuai ukuran *Maximum Transmission Unit* (*MTU*) yang telah distandarkan. *MTU* adalah ukuran maksimal dari sebuah data yang dapat di

transmisikan dalam 1 paket. Apabila ukuran data yang dikirimkan melebihi dari ukuran *MTU* maka data tersebut akan dipecah menjadi beberapa paket. Semakin besar ukuran *MTU* maka jumlah paket yang melalui jaringan komputer akan semakin sedikit namun dapat memuat informasi yang banyak. Namun apabila paket tersebut rusak maka banyak data yang akan hilang. Sebaliknya apabila ukuran *MTU* kecil, jumlah paket yang melalui jaringan komputer akan banyak namun memuat data yang sedikit. Dan apabila terjadi kerusakan pada paket yang dikirimkan, data yang hilang tidak terlalu banyak. Maka penentuan ukuran *MTU* akan berkorelasi secara langsung kepada performa jaringan komputer.

e. Layer 3 – Network Layer

Lapisan ini mengatur tentang alamat *Internet Protocol* (*IP Address*) dari sebuah perangkat yang terhubung ke jaringan komputer. *IP Address* merupakan identitas dari perangkat yang terhubung ke jaringan komputer sehingga pertukaran data dapat dilakukan. Secara umum *IP Address* dibagi menjadi 2 kelompok yaitu *IP Address Public* dan *Local*. *IP Address Public* adalah alamat sebuah perangkat jaringan komputer (*server* / *router*) yang dapat diakses secara langsung melalui koneksi internet. Alokasi *IP Address* diatur oleh IANA (*Internet Assigned Numbers Authority*) yaitu sebuah lembaga yang mengatur alokasi *IP Public* di seluruh dunia. Hal ini perlu dilakukan karena *IP Address* merupakan salah satu informasi yang harus diketahui oleh perangkat komputer sebelum terjadinya pengiriman data. Sedangkan *IP Private* diatur oleh *computer network administrator* dari masing-masing lembaga yang memiliki jaringan komputer. Maka sangat dimungkinkan untuk menggunakan *IP Address* yang sama di beberapa lembaga yang berbeda. Namun hal ini tidak menjadi permasalahan karena paket data yang dikirimkan akan melalui proses *routing* terlebih dahulu.

f. Layer 2 – Data Link Layer

Data Link Layer merupakan lapisan yang akan memberikan informasi *Media Access Control (MAC) Address* pada paket data yang melalui lapisan ini. *MAC Address* merupakan identitas dari *Network Card* yang terdiri dari 48-bit angka heksadesimal. 6 bit pertama dari *MAC Address* merupakan informasi dari pembuat *Network Card* dan sisanya merupakan kode unik dari *Network Card*

tersebut. Informasi *MAC Address* akan disimpan di perangkat yang terhubung ke jaringan komputer seperti komputer, *router* , *switch* dll yang disebut dengan tabel *Address Resolution Protocol* (*ARP*)

g. Layer 1 – Physical Layer

Pada layer terendah dari *OSI Layer*, *Physical layer* menerima data dari *Data Link layer* dan mengubahnya menjadi sinyal pada media transmisi. Tergantung dari media transmisi yang digunakan, apabila menggunakan media transmisi kabel *UTP* maka *frame* / *PDU* akan diubah menjadi arus listrik DC. Apabila menggunakan media transmisi *Fiber Optic* maka *frame* / *PDU* akan diubah menjadi cahaya. Sedangkan apabila menggunakan media transmisi nirkabel maka *frame* / *PDU* akan diubah menjadi gelombang radio.

2.5.2. *Transmission Control Protocol* (*TCP*) *Layer*

Menurut Prakasa (2019), pada dasarnya model komunikasi data yang di usulkan pada awal pengembangan jaringan komputer adalah *Transmission Control Protocol Layer* yang kemudian berkembang menjadi *Internet Protocol*, maka kemudian lebih banyak disebut dengan *TCP*/*IP Layer*. Perbedaan utama dari *TCP*/*IP* Layer dengan *OSI Layer* adalah apabila *TCP*/*IP Layer* dibagi menjadi 4 lapisan sedangkan *OSI Layer* dibagi menjadi 7 lapisan. Meskipun *TCP*/*IP Layer* hanya terdiri dari 4 lapisan, namun *TCP*/*IP Layer* yang digunakan pada implementasi jaringan komputer di dunia nyata. Hal ini karena *TCP*/*IP Layer* dikembangkan bersama dengan pengembangan jaringan komputer itu sendiri. Sehingga standar – standar yang diusulkan pada *TCP*/*IP Layer* yang digunakan oleh industri perangkat jaringan komputer. Sedangkan *OSI Layer* digunakan lebih untuk mempermudah proses pembelajaran tentang jaringan komputer.

2.6. Protokol

Menurut Prakasa (2019), *protokol* merupakan aturan komunikasi data yang dibuat dan disepakati bersama oleh para pengembang jaringan komputer. Tujuan dari dibuatnya *protokol* ini adalah agar terjadi sebuah standar komunikasi data tanpa memandang perangkat / pabrikan yangmenggunakan protokol tersebut. Hasilnya

adalah jaringan komputer yang ada saat ini meskipun terdiri dari berbagai perangkat keras dan perangkat lunak namun dapat berkomunikasi dengan baik karena adanya protokol.Beberapa protokol dasar yang sering digunakan dan perlu diketahui khususnyadari sisi jaringan komputer adalah sebagai berikut :

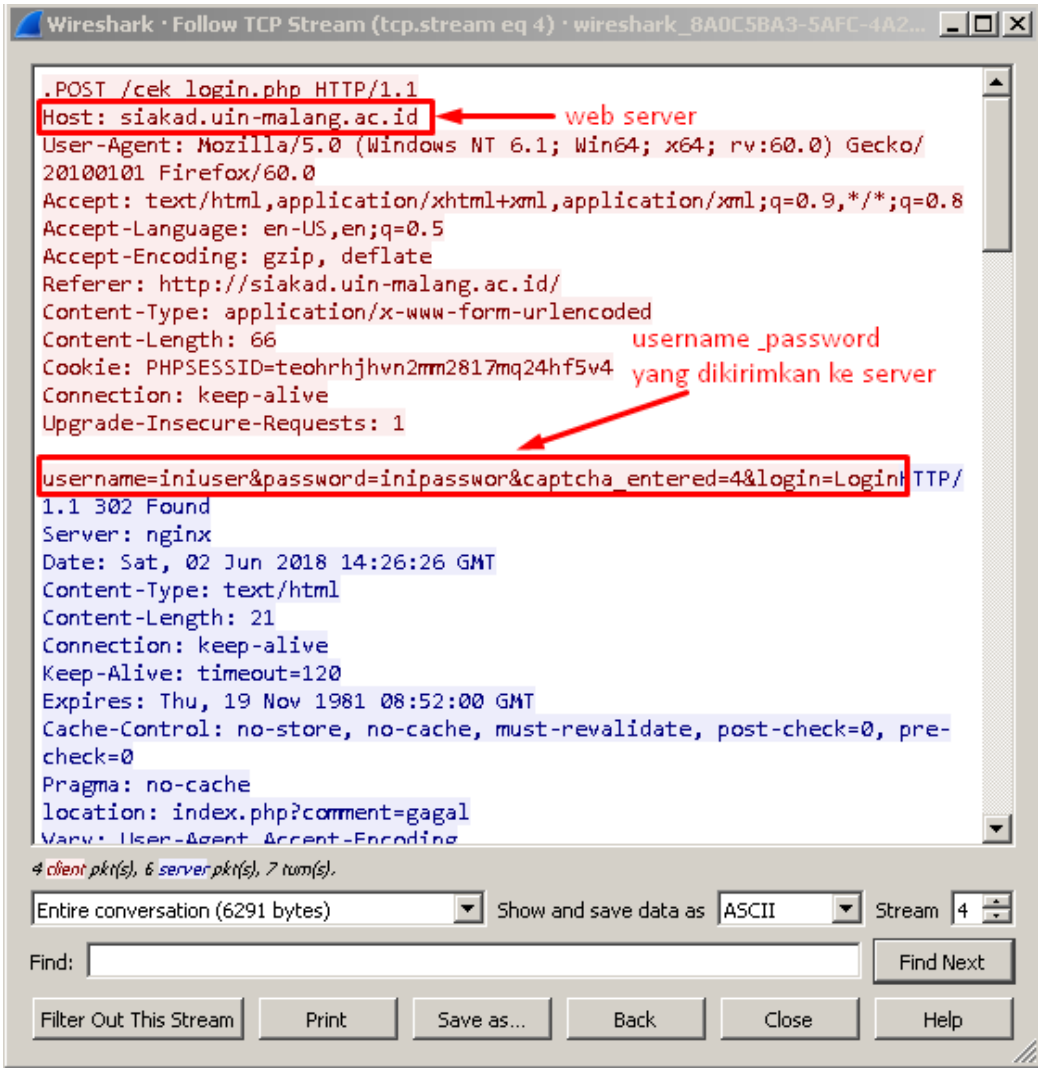
2.6.1. Hyper Text Transfer Protocol (HTTP)

Menurut Prakasa (2019), *HTTP* diusulkan pada dokumen RFC 1945 dan 2616 dimana berfungsi untuk komunikasi data *website* dan digunakan sejak tahun 1990 dimana pertama kali jaringan *internet* dapatdiakses oleh masyarakat luas.

HTTP merupakan protokol berjenis *request / response* dimana komputer *client* harus mengirimkan *request* halaman *website* ke *web server* untuk kemudian di *response* oleh *web server* dengan mengirimkan halaman yang diminta. Secara *default HTTP* akan menggunakan *port* 80 dan tidak disarankan untuk diubah (meskipun bisa diubah) karena sudah menjadi *port* standar *web server* (*web browser*secara *default* akan mengakses *port* 80 pada *server*).

Untuk mendapatkan data dari *server*, *client* akan mengirimkan data dengan metode *GET* sedangkan untuk mengirimkan respon (balasan) *client* akan mengirimkan data dengan metode *POST*. Diantara metode tersebut komunikasi *client* dengan *server* akan terputus (tidak terus dijaga) sehingga memungkinkan sebuah *web server* dapat melayani permintaan data dari banyak *client* pada waktu yang hampir bersamaan.

Namun kelemahan dari protokol HTTP adalah pengiriman data dari *client* ke *server* atau sebaliknya dilakukan secara *plain text* atau tidak di sandikan (*enkripsi*). Hal ini menjadikan protokol *HTTP* tidak aman dan sering dijadikan sasaran pencurian data sensitif seperti *username* dan *password* sebuah *website* dengan cara *sniffing* pada jaringan komputer. Pada Gambar 2.18 di bawah ini ditunjukkan hasil *sniffing* pada protokol dimana *username* dan *password* yang dikirimkan dari *client* ke *server* dapat terlihat dengan jelas :



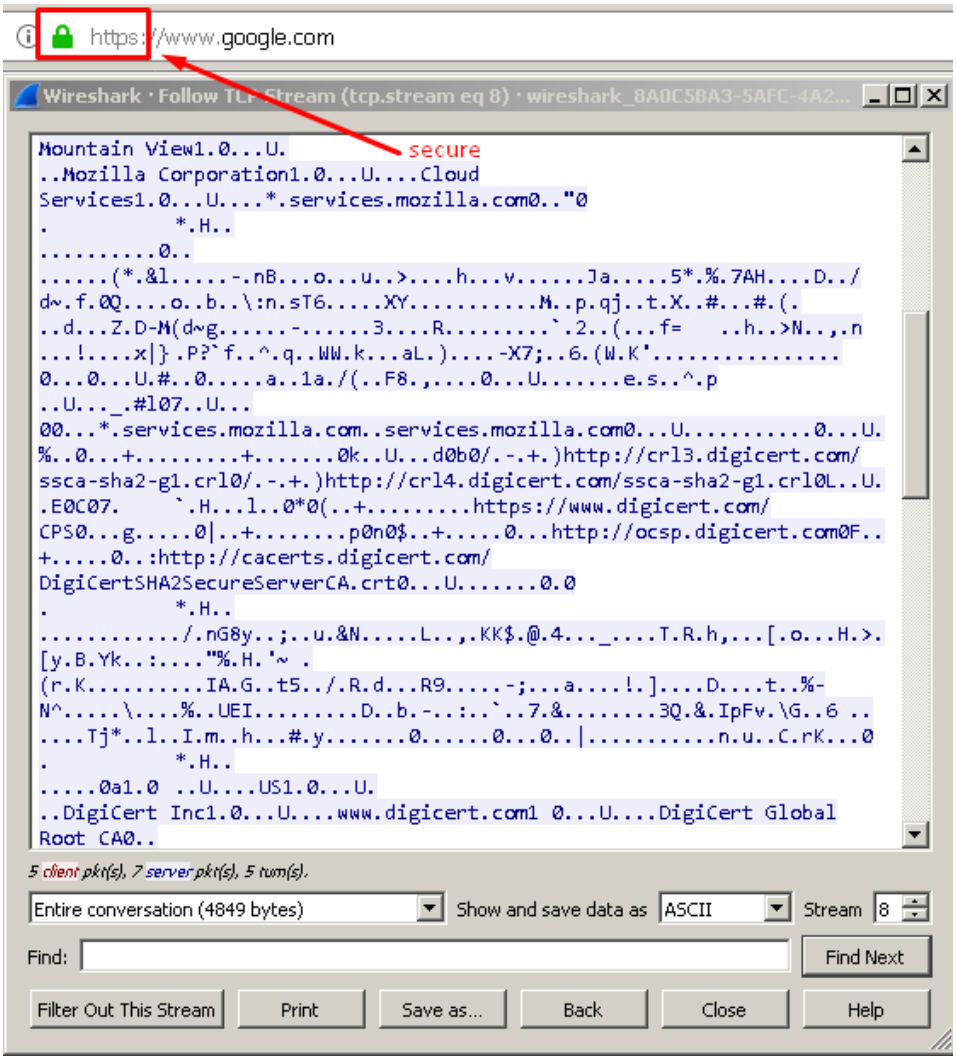
Sumber : Prakasa(2019)

Gambar 2. 18. *Sniffing HTTP Protocol*

2.6.2. Hyper Text Transfer Protocol Secure (HTTPS)

Menurut Prakasa (2019), *HTTPS* dikembangkan menyusul sangat rentannya protokol *HTTP* dari segi keamanan yang diusulkan pada *RFC* 2660. Apabila pada protokol *HTTP* data dikirimkan secara *plain text* (sehingga dapat di *sniffing*) maka pada *HTTPS* data akan dikirimkan di atas protokol *SSL* (*Secure Socket Layer*). *SSL* bertugas untuk melakukan *enkripsi* dan *dekripsi* data di sisi *client* dan *server* sehingga pada dasarnya *client* dan *server* tetap berkomunikasi menggunakan protokol *HTTP*. *SSL* memastikan bahwa *server* mengirimkan data ke *client* yang benar dan *client* mengirimkan data ke *server* yang benar. Karena sebelum pengiriman data dimulai,

terlebih dahulu akan terjadi pertukaran *encryption key* antara *client* dan *server*. Hal ini untuk menghindari *sniffing* sehingga data yang melalui jaringan komputer sudah dalam kondisi tersandikan (*encrypted*). Pada Gambar 2.19 terlihat bahwa *traffic HTTPS* tidak dapat di *sniffing* di jaringan komputer karena sudah dalam kondisi tersandikan (*encrypted*).



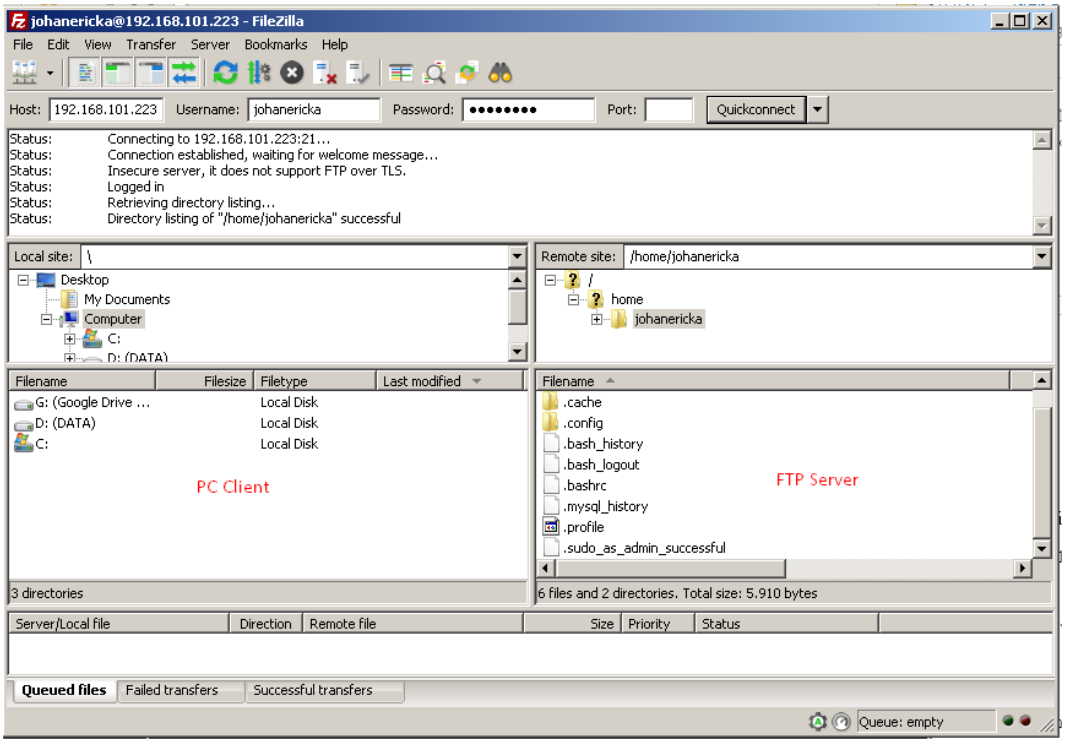
Sumber : Prakasa(2019)

Gambar 2. 19. *Sniffing HTTPS Protocol*

2.6.3. File Transfer Protocol (FTP)

Menurut Prakasa (2019), *FTP* merupakan protokol yang digunakan untuk mengirimkan *file sharing*. *FTP Server* merupakan *server* tempat dimana *file* disimpan. Untuk dapat mengakses *file* yang ada di *FTP Server*, dibutuhkan *username* dan *password* sehingga sebuah direktori pada *FTP Server* hanya diperuntukkan seorang

user dan tidak dapat diakses oleh *user* lainnya (kecuali diberikan hak akses / diijinkan). Gambar 2.20 menunjukkan akses ke *FTP server* menggunakan program *FTP Client File Zilla.* Secara *default FTP* menggunakan *port* 21 dan disarankan untuk diubah ke *port* lain untuk mengaburkan layanan *FTP* yang aktif di sebuah komputer / *server*.



Sumber : Prakasa (2019)

Gambar 2. 20. Akses ke *FTP Server*

2.6.4. Domain Name System (DNS)

Menurut Prakasa (2019), *Domain Name System* merupakan sebuah sistem yang bertugas untuk menterjemahkan *IP Address* dari sebuah *server* menjadi nama domain dengan tujuan agar lebih mudah diingat oleh manusia. Apabila untuk mengidentifikasi manusia menggunakan Nama, maka perangkat yang terhubung ke jaringan komputer diidentifikasidengan menggunakan *IP Address*. Karena *IP Address* merupakan sekumpulan angka–angka dimana akan menyulitkan manusia untuk mengingatnya maka diciptakanlah *Domain Name System* sebagai kamus yang menterjemahkan nama domain dari sebuah*server* menjadi *IP Address*. Hal ini diperlukan karena komunikasi komputer yang terhubung ke jaringan menggunakan *IP Address* sedangkan manusia

lebih mudah menggunakan nama (*domain name*). Secara *default DNS* menggunakan *port* 53. *DNS* menggunakan *UDP* karena paket yang dikirimkan relatif kecil dan bersifat pemberitahuan (memberitahu *client* tentang *IP* dari domain yang dituju) sehingga dapat dianggap tidak terlalu penting (dapat dilakukan pengiriman ulang apabila paket rusak di tengah jalan).Namun saat ini karena ukuran dari paket data yang dikirimkan semakin membesar maka pada beberapa kasus *DNS* menggunakan protokol *TCP*.

2.6.5. Transmission Control Protocol (TCP)

Menurut Prakasa (2019), *Transmission Control Protocol (TCP)* merupakan protokol standar komunikasi data pada perangkat yang terhubung ke jaringan komputer. Dengan menggunakan *TCP*, aplikasi tidak perlu memotong data sebelum dikirimkan. Pemotongan data akan dikerjakan oleh *TCP*. *TCP* menggunakan teknik *connection-oriented* dimana pengiriman data dapat diandalkan. Teknik ini akan mengirimkan urutan data pada paket data yang dikirimkan sehingga perangkat penerima dapat mengetahui urutan dari paket data yang diterima. Dengan menggunakan teknik diatas akan dapat mengetahui paket data yanggagal dikirim sehingga akan dikirimkan ulang. Pihak penerima dapat mengetahui paketmana yang belum diterima dan akan mengirimkan permintaan *retransmission*.

2.6.6. User Datagran Protocol (UDP)

Menurut Prakasa (2019),*UDP* menggunakan teknik *connectionless*. Teknik ini tidak memelihara koneksi antara perangkat yang berhubungan atau *send and forget*. Segera setelah paket data dikirimkan maka koneksi dengan perangkat tujuan akan diputus. Oleh karena itulah *UDP* digunakan untuk mengirim data yang relatif kecil dan bersifat *real Time* serta satu arah. Salah satu implementasi *UDP* yang paling terkenal adalah pada komunikasi *DNS*. Implementasi lain dari *UDP* adalah pada paket *streaming* (*VOIP* / Video) yaitu pengiriman data berupa suara / gambar.

2.6.7. *Internet Control Message Protocol (ICMP)*

Menurut Prakasa (2019), *ICMP* merupakan salah satu protokol di jaringan komputer yang paling banyak dikenal karena digunakan pada ping. *ICMP* digunakan untuk melakukan pengecekan terhadap jaringan komputer apakah jalur ke perangkat yang akan dituju tersambung atau tidak.

2.6.8. Addres Resolution Protocol (ARP)

Menurut Prakasa (2019), *ARP* bertugas untuk memetakan informasi *IP Address* ke *MAC Address* perangkat yang terhubung ke jaringan komputer. Hal ini diperlukan karena pada *OSI Layer* telah dijelaskan bahwa pengiriman data pada *Layer* 2 membutuhkan *MAC Address* perangkat yang dituju.

2.7. *IP Address*

Menurut Madcom (2015), *IP Address* atau alamat IP adalah alamat yang diberikan ke jaringan dan peralatan jaringan yang menggunakan *protocol TCP*/*IP*. *IP Address* terdiri dari 32 bit angka biner yang dapat dituliskan sebagai desimal yang dipisahkan oleh tanda titik seperti 192.168.10.1 oleh karena *protocol IP* adalah *protocol* yang paling banyak dipakai untuk keperluan *routing* informasi di dalam jaringan komputer satu dengan yang lain.

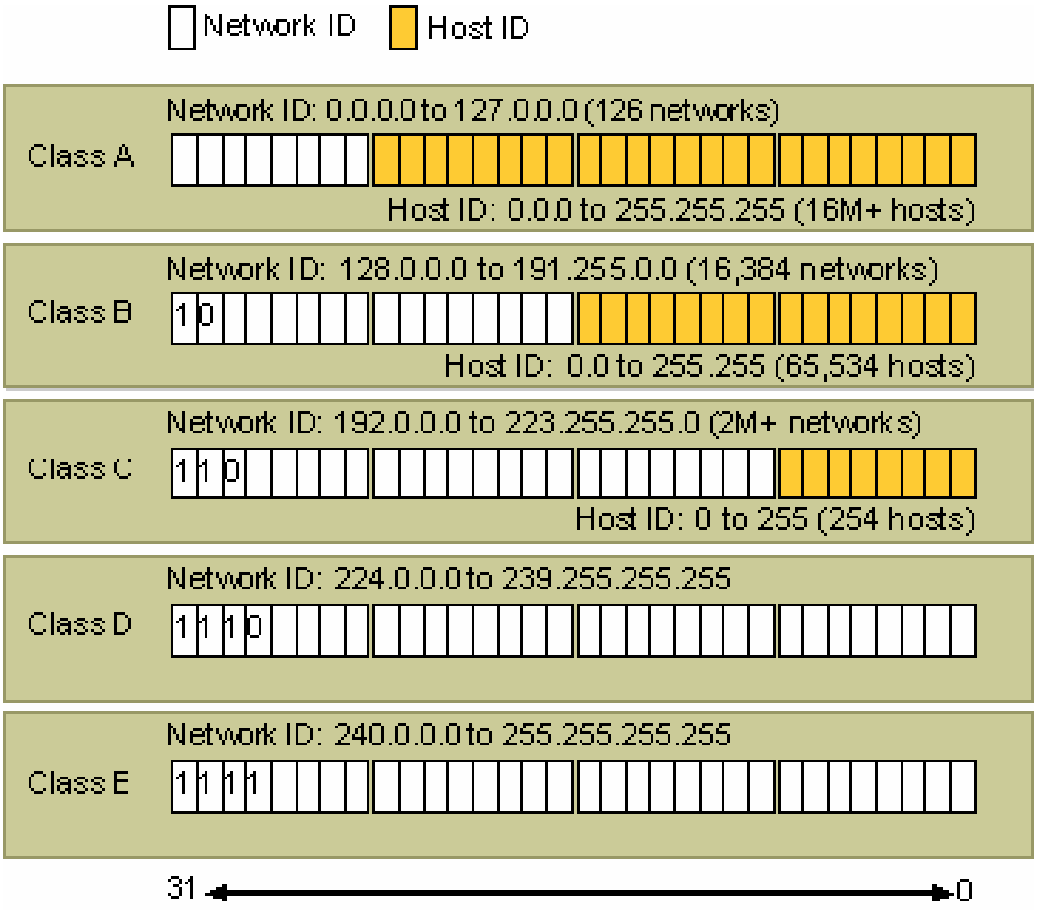
2.7.1. IP Addresss versi 4

Menurut Prakasa (2019), *IP Address* yang umum digunakan saat ini adalah *IP Address* versi 4 dimana versi 1 s/d 3 hanya merupakan konsep (tidak dapat di implementasikan). *IP Address* versi 4 terdiri dari 32 bit angka biner yang merepresentasikan sebuah angka tertentu yang akan dijadikan sebagai identitas perangkat yang terhubung ke jaringan. Angka–angka biner tersebut dikelompok-kan menjadi 4 kelompok yang dipisahkan dengan titik (*dot*) dimana masing–masing kelompok memiliki 8 bit angka biner dimulai dari 00000000 = 0 sampai 11111111 = 255. Sehingga nilai dari sebuah *IP Address* berada di antara 00000000.00000000.00000000.00000000 (0.0.0.0) = 0 dan 11111111.11111111.11111111.11111111 (255.255.255.255). Maka (secara teori) maksimal jumlah *host* / perangkat jaringan yang dapat menggunakan *IP Public* adalah (255 x 255 x 255 x 255) = 4.294.967.296 perangkat.

2.7.2. IP Addresss Classes

Menurut Prakasa (2019), badan yang bertanggung jawab tentang distribusi *IP Public* adalah *IANA* (*Internet Assigned Number Authority*), *IP Address* dibagi menjadi 5 kelas yaitu kelas A, B, C, D (*multicast*) dan E (*reserved*) yang disebut dengan *Classfull Address*. *IP Address* terdiri dari *Network* dan *Host* seperti pada Gambar 2.21

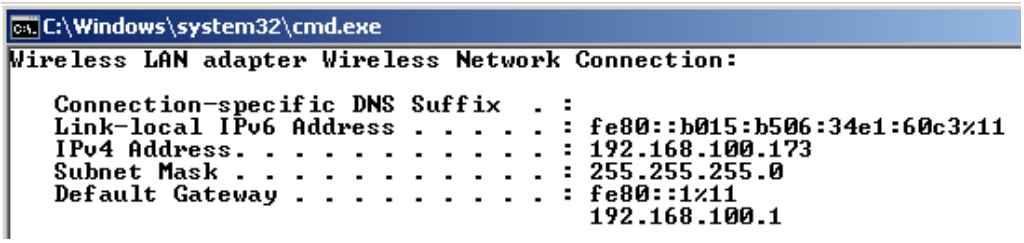
berikut ini :



Sumber : Prakasa(2019)

Gambar 2. 21. *Network* dan *Host*

Network merupakan kumpulan dari perangkat jaringan komputer yang saling terhubung. Sedangkan *host* adalah nomor dari perangkat jaringan komputer. Untuk mempermudah pemahaman tentang *host* dan *network* dapat dianalogikan seperti kawasan perumahan. *Network* dapat dianalogikan seperti jalan perumahan sedangkan *host* dapat dianalogikan seperti rumah yang ada di jalan tersebut. Maka dalam sebuah *network* dapat terdiri dari banyak *host.* Data yang dikirimkan harus memuat informasi tentang *network* dan *host* yang dituju. Jalan untuk keluar masuk ke sebuah *network* disebut dengan *Gateway*. Sedangkan untuk mengidentifikasi kelas dari sebuah *network* dibutuhkan *Subnet.* Berikut contoh dari *IP Address, Subnet* dan *Gateway* pada sebuah komputer yang terhubung ke jaringan.



Sumber : Prakasa(2019)

Gambar 2. 22. *IP Address* pada *Wireless card*

Pada Gambar 2.22 di atas tampak sebuah *Wireless LAN* Adapter memiliki *IP Address* 192.168.100.173, *Subnet Mask* 255.255.255.0 dan *Gateway* 192.168.100.1. Angka-angka tersebut adalah identitas dari sebuah perangkat yang terhubung ke jaringan komputer yang digunakan untuk mengirim / menerima data.

2.7.3. Notasi IP Addresss v4

Menurut Prakasa (2019), sebuah *IP Address* versi 4 terdiri dari 4 oktet yang dipisahkan dengan tanda titik. Masing–masing oktet dapat memiliki nilai antara 0 s/d 255. Namun komputer membaca *IP Address* tidak dalam format desimal melainkan dalam format biner (0 dan 1). Untuk menterjemahkan *IP Address* di atas menjadi format biner, dapat dilakukan dengan Tabel 2.2 sebagai berikut :

Tabel 2.2. Konversi *IP* ke *biner*

128	64	32	16	8	4	2	1
0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1

Tabel 2.2 diatas adalah tabel yang berisi nilai 1 oktet dari *IP Address*. Sehingga pada contoh diatas nilai 192 (desimal) dapat di konversi menjadi 11000000. Caranya adalah dengan memberikan nilai 1 pada nilai yang paling mendekati nilai desimalnya, dalam hal ini 128 + 64 = 192. Karena nilai 192 sudah tercapai maka sisanya akan diisi dengan 0. Dengan cara yang sama, *IP Address* diatas apabila dikonversi menjadi bilangan biner akan menjadi

192	.	168	.	100	.	173
11000000	.	10101000	.	01100100	.	10101101

Untuk memudahkan dalam penggunaannya, *IP Address* dibagi menjadi beberapa

kelas. Masing–masing kelas memiliki jumlah *network* dan *host* yang berbeda. Semakin tinggi kelas *IP Address*, maka jumlah *host* yang dapat ditampung akan semakin banyak dan sebaliknya semakin rendah kelas *IP Address* maka jumlah *host* yang dapat ditampung dalam sebuah *sub-network* tersebut semakin sedikit. Berikut pembagian kelas *IP Address* beserta *subnet* dan *host* yang dapat ditampung di *subnet* tersebut :

Tabel 2. 3. *IP Address v4 Classes*

Kelas	IP Awal	IP Akhir	Network ID (maks)	Host ID (maks)	*Subnet* Mask
A	0.0.0.0	126.255.255.255	128 (2^7)	16.777.216 (2^{24})	255.0.0.0
	127.0.0.0	127.255.255.255	*loopback*		
B	128.0.0.0	191.255.255.255	16.384 (2^{14})	65.536 (2^{16})	255.255.0.0
C	192.0.0.0	223.255.255.255	2.097.152 (2^{21})	256 (2^8)	255.255.255.0
D	224.0.0.0	239.255.255.255	Multicast		
E	240.0.0.0	255.255.255.255	Eksperiment		

Dari Tabel 2.3 diatas dapat diketahui bahwa *IP* Kelas A memiliki *sub-network* yang cukup sedikit dan jumlah *host* yang sangat banyak. Efek dari penggunaan *subnet* dalam skala yang besar akan terjadi pengiriman *hello message* secara *broadcast* yang besar pula. *Hello message* adalah paket data yang dikirimkan untuk mencari *host* yang dituju apakah terdapat di dalam *subnet* tersebut atau di luar *subnet*. *Hello message* dikirimkan secara *broadcast* dimana pada *subnet* besar akan dapat terjadi efek *broadcast storm* yang akan dapat melumpuhkan jaringan itu sendiri. Maka penentuan besar *subnet* dapat berpengaruh terhadap performa jaringan komputer itu sendiri.

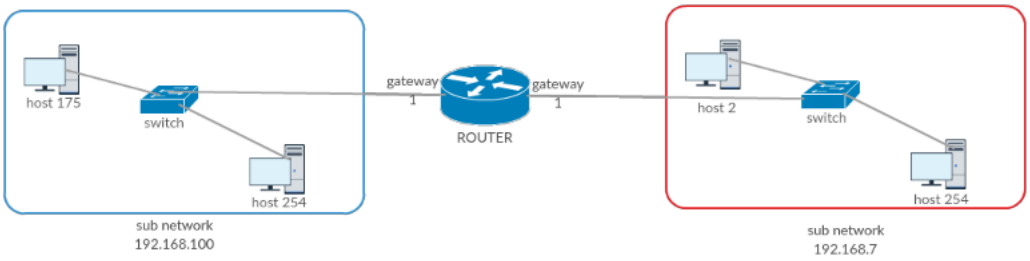
2.7.4. Perhitungan IP Addresss v4

Menurut Prakasa (2019), *Subnetting* adalah istilah yang sering digunakan untuk membagi jaringan komputer menjadi beberapa sub - jaringan komputer yang lebih kecil dengan tujuan untuk memudahkan manajemen jaringan komputer, meningkatkan

keamanan serta membatasi akses terhadap jaringan komputer. Pada jaringan komputer dikenal beberapa istilah yang akan dijelaskan di bawah ini :

a. *Network address* adalah alamat yang menunjukkan jaringan komputer tertentu. Maka *network address* termasuk didalam *IP Address* perangkat untuk mengidentikasi perangkat tersebut termasuk pada bagian jaringan komputer tertentu. Pada contoh *IP Address* di atas 192.168.100.173 (kelas C) yang merupakan *network address* adalah 192.168.100 (3 oktet pertama merupakan *network address*).*Gateway address* atau sering disebut dengan *Gateway* saja merupakan alamat untuk menuju / dari sub *network* tertentu. Sehingga perangkat pada *sub network* lain hanya perlu mengetahui alamat dari *Gateway sub network* yang akan menerima datanya. Pada contoh diatas *Gateway Address* adalah 192.168.100.1.
b. *Host address* adalah alamat yang menunjukkan alamat dari sebuah perangkat di dalam jaringan komputer tersebut. Pada contoh *IP Address* di atas 192.168.100.173 (kelas C) yang merupakan *host address* adalah 173 (oktet terakhir merupakan *host* address).
c. *Subnet Mask* adalah *IP Address* yang menunjukkan jumlah *host* yang terdapat di dalam jaringan tersebut. Untuk kelas C *Subnet Mask* nya adalah 255.255.255.0 dimana dapat diartikan pada *subnet* tersebut dapat menampung sebanyak 255 *host*.
d. *Broadcast address* adalah *IP Address* yang digunakan untuk mengirimkan data ke semua *host* yang ada di dalam jaringan tersebut. Biasanya digunakan untuk mencari apakah *host* tertentu di dalam sub *network* tersebut. Misalnya pada *DHCP Discover* (ketika *host* melakukan pencarian *DHCP Server* di dalam sebuah sub *network* untuk mendapatkan informasi tentang sub *network* secara otomatis). Biasanya merupakan *IP Address* terakhir yang ada didalam *subnet* tersebut.

Apabila digambarkan secara visual, maka jaringan istilah – istilah diatas dapat digambarkan seperti pada Gambar 2.3 di bawah ini :



Sumber : Prakasa(2019)

Gambar 2. 23. Network address

Seperti yang telah dijelaskan sebelumnya bahwa fungsi dari *switch* adalah untuk menghubungkan perangkat pada sub *network* yang sama. Sedangkan fungsi *router* adalah untuk menghubungkan perangkat pada sub *network* yang berbeda. *Gateway* adalah *IP Address* pertama yang ada di *sub network* tersebut dan pada teknis nya diletakkan pada *router* sehingga *router* dapat mengetahui *sub network* berapa saja yang dapat dijangkaunya serta melakukan proses *routing* (mengetahui jalur pengiriman data).

2.7.5. Classless Inter Domain Routing (CIDR)

Menurut Prakasa (2019), *CIDR* merupakan salah satu cara untuk menggambarkan besarnya *subnetwork*. Apabila pada *Classfull IP Address* hanya dibagi menjadi 3 kelas (A, B dan C) maka pada *CIDR* dapat didefinisikan *sub-network* lebih banyak lagi sehingga tidak terjadi pemborosan *IP Address*.

CIDR merupakan cara penulisan *Subnet Mask* dari sebuah *subnetwork* dengan cara mengubah notasi *subnetwork* dari desimal ke biner kemudian menghitung jumlah nilai biner 1 yang ada. Langkah–langkah untuk mengubah notasi *subnetwork* desimal menjadi biner adalah sebagai berikut. Misal pada sub *network ClassfullIP Address* kelas C dituliskan 255.255.255.0 maka apabila nilai 255 diubah menjadi bilangan biner (8 oktet) adalah 11111111. Maka untuk sub *network* kelas C apabila di tuliskan dalam bentuk binernya adalah 11111111.11111111.11111111.00000000 dengan jumlah angka 1 sebanyak 24. Maka notasi *subnetwork* kelas C pada *CIDR* dituliskan dalam /24 (terdapat 24 biner 1).

Berikut ini adalah Tabel 2.4 daftar *subnetwork* dalam notasi desimal dan biner (*CIDR*).

Tabel 2. 4. Daftar *Sub Network*

Classfull IP Address	Subnet Mask	Notasi CIDR	Jumlah Host
A	128.0.0.0	/1	2.147.483.646
	192.0.0.0	/2	1.073.741.822
	224.0.0.0	/3	536.870.910
	240.0.0.0	/4	268.435.454
	248.0.0.0	/5	134.217.726
	252.0.0.0	/6	67.108.862
	254.0.0.0	/7	33.554.430
	255.0.0.0	/8	16.777.214
	255.128.0.0	/9	8.388.606
	255.192.0.0	/10	4.194.302
	255.224.0.0	/11	2.097.150
	255.240.0.0	/12	1.048.574
	255.248.0.0	/13	524.286
	255.252.0.0	/14	262.142
	255.254.0.0	/15	131.070
B	255.255.0.0.	/16	65.534
	255.255.128.0	/17	32.766
	255.255.192.0	/18	16.382
	255.255.224.0	/19	8.190
	255.255.240.0	/20	4.094
	255.255.248.0	/21	2.046
	255.255.252.0	/22	1.022
	255.255.254.0	/23	510
C	255. 255. 255.0	/24	254
	255. 255. 255.128	/25	126
	255. 255. 255.192	/26	62
	255. 255. 255.224	/27	30
	255. 255. 255.240	/28	14
	255. 255. 255.248	/29	6
	255. 255. 255.252	/30	2

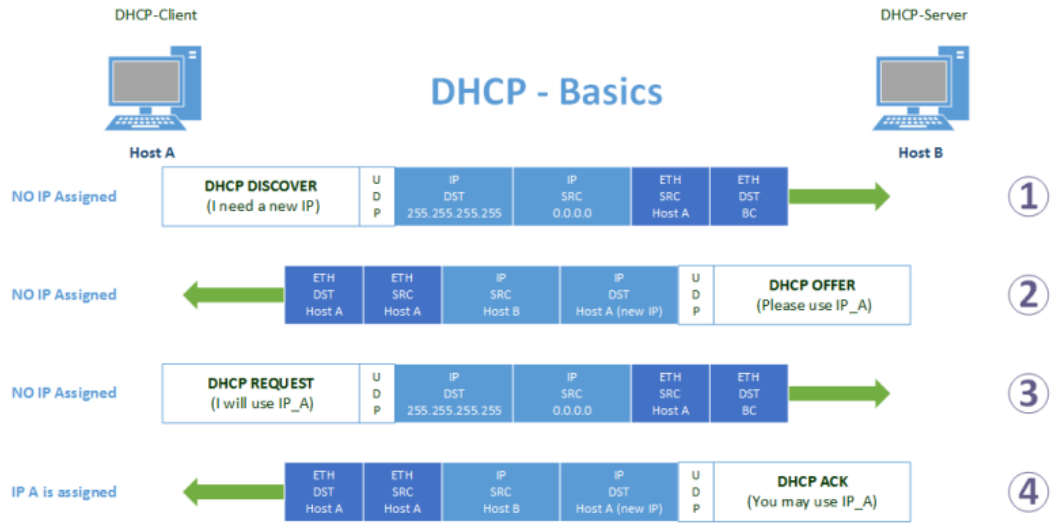
2.7.6. *Variable Lenght Subnet Mask (VLSM)*

Menurut Prakasa (2019), *Variable Length Subnet Mask* (*VLSM*) merupakan cara untuk membagi jaringan komputer menjadi lebih kecil (sub-*net*) atau lebih besar (super-*net*) sesuai kebutuhan. Permasalahan pada *classfull IP* adalah hanya tersedia 3 kelas *IP* yang dapat digunakan (A, B dan C) sedangkan kebutuhan di lapangan seringkali tidak sebanyak itu dimana yang paling sedikit adalah kelas C yang mampu menampung 254 perangkat jaringan komputer. Apabila hal ini diterapkan pada *IP*

Public maka akan sangat boros *IP*. Dengan menggunakan *VLSM* maka dimungkinkan untuk membagi *subnetwork* kelas C menjadi beberapa *subnetwork* yang lebih kecil lagi. Dengan demikian apabila dibutuhkan untuk membuat jaringan komputer yang hanya berisi 12 perangkat cukup menggunakan sub *network* /28 atau 255.255.255.240 . Dengan demikian maka slot *IP Address* yang tidak terpakai pada sub *network* tersebut dapat diminimalisir.

2.7.7. *Dynamic Host Configuration Protocol (DHCP)*

Menurut Prakasa (2019), *Dynamic Host Configuration Protocol* merupakan protokol untuk memberikan informasi tentang jaringan komputer (*IP Address*, *Subnet* , *Gateway*, *DNS* dll) kepada perangkat lain yang terhubung ke jaringan komputer secara otomatis. Dengan demikian perangkat yang terhubung ke jaringan komputer tidak perlu melakukan konfigurasi jaringan komputer secara manual.



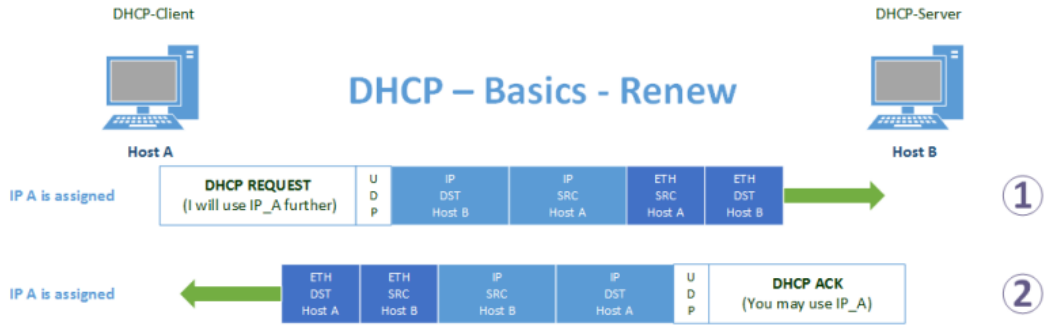
Sumber : Prakasa(2019)

Gambar 2. 24. *DHCP basics*

Pada Gambar 2.24 diatas menjelaskan proses yang terjadi ketika sebuah perangkat (komputer) terhubung ke jaringan yang memiliki *DHCP Server*. Pertama terhubung ke jaringan komputer, layanan *DHCP Client* yang ada di komputer akan mengirimkan pesan *broadcast* untuk mencari apakah di jaringan tersebut memiliki *DHCP Server*. Apabila jaringan tersebut memiliki *DHCP Server* maka *DHCP Server* akan mengirimkan balasan berupa seperangkat informasi jaringan komputer (*IP Address*, *Subnet* , *Gateway* dll) secara *unicast* (pada saat ini *DHCP Server* telah mengetahui

Mac Address yang dikirimkan komputer *client*). Informasi ini dikenal dengan nama *DHCP Offer*. Apabila komputer *client* bersedia menggunakan informasi tersebut maka komputer *client* akan mengirimkan pesan yang dinamakan *DHCP Acknowledge* kepada *DHCP Server*.

Sehingga di *DHCP Server* akan dicatat bahwa *Mac Address* komputer *client* mengajukan *IP Address* tertentu selama waktu tertentu (disebut *lease time*). *Lease time* merupakan waktu tertentu yang diberikan kepada sebuah perangkat dalam menggunakan *IP Address*. Apabila *lease time* sudah mendekati waktu habis namun komputer *client* masih terhubung ke jaringan komputer, maka komputer *client* secara otomatis akan mengirimkan paket *DHCP Renew* yang bertujuan untuk memberitahu kepada *DHCP Server* agar menambah waktu penggunaan *IP Address* oleh komputer *client*. Dengan demikian selama komputer *client* terhubung ke jaringan maka *IP Address* akan selalu digunakan. Ilustrasi proses diatas digambarkan pada Gambar 2. 25 berikut ini :



Sumber : Prakasa(2019)

Gambar 2. 25. *DHCP renew*

2.7.8. *IP Public vs IP Lokal*

Menurut Prakasa (2019), *IP Public* merupakan *IP Address* yang dapat di akses langsung dari internet. Biasanya digunakan untuk server agar dapat diakses dari manapun selama terhubung ke internet. Penggunaan *IP Public* diatur oleh *IANA* (*Internet Assigned Number Authority*) yaitu sebuah lembaga yang mengatur tentang penggunaan *IP Public*. Dengan demikian dapat dipastikan bahwa *IP Public* hanya digunakan untuk 1 perangkat saja (tidak terduplikasi).

Untuk memanajemen *IP Address* di wilayah Asia Tenggara (termasuk Indonesia),

IANA diwakili oleh *APNIC* (*Asia Pasific Network Information Center*). Di Indonesia sendiri telah dibentuk *IDNIC* (*Indonesian Network Information Center*) sebagai "*Country NIC*" sehingga perusahaan yang membutuhkan *IP Public* tidak perlu langsung ke *APNIC* melainkan cukup ke *IDNIC* (sebagai perpanjangan tangan *APNIC* di Indonesia).Gambar 2. 26 Ilustrasi Pembagian Wilayah Pengelola *IP*

Sumber : Prakasa(2019)

Gambar 2. 26. Ilustrasi Pembagian Wilayah Pengelola IP

Karena keterbatasan *IP Public* serta tidak semua komputer perlu dapat diakses melalui jaringan internet, maka dikembangkan *IP Private*. *IP Private* adalah *IP Address* yang dialokasikan untuk perangkat-perangkat di dalam internal organisasi / jaringan komputer lokal. Maka yang bertanggung jawab memanajemen *IP Private* adalah *Network Administrator* perusahaan. Dan karena terletak di internal perusahaan, maka sangat dimungkinkan *IP Address* di suatu perusahaan ternyata sama dengan yang digunakan di perusahaan lainnya. Namun hal ini tidak menjadikan sebuah masalah karena kedua jaringan komputer akan melalui *router* terlebih dahulu dan komputer di internet hanya akan mengetahui *IP Address* dari *router* (*gateway*) yang digunakan. Maka secara teknis hanya dibutuhkan 1 *IP Public* sebagai jalur komunikasi ke internet, untuk semua komputer yang ada di perusahaan

2.8. Sekretariat Daerah Kota Salatiga (Setda Salatiga)

Berdasarkan Peraturan Walikota Salatiga Nomor 24 Tahun 2016 tentang kedudukan, susunan organisasi, tugas dan fungsi serta tata kerja sekretariat daerah Sekretariat Daerah Kota Salatiga (Setda Salatiga) merupakan perangkat daerah dari unsur staf yang dipimpin oleh Sekretaris Daerah yang berkedudukan di bawah dan bertanggung jawab kepada Walikota.

2.8.1. Tugas Sekretariat Daerah Kota Salatiga

Sekretariat Daerah mempunyai tugas membantu Walikota dalam penyusunan kebijakan dan pengoordinasian administratif terhadap pelaksanaan tugas perangkat daerah serta pelayanan administratif.

2.8.2. Fungsi Sekretariat Daerah Kota Salatiga

Sekretariat Daerah mempunyai fungsi sebagai berikut :

a. Pengoordinasian penyusunan kebijakan Daerah
b. Pengoordinasian pelaksanaan tugas Perangkat Daerah
c. Pemantauan dan evaluasi pelaksanaan kebijakan Daerah
d. Pelayanan administratif dan pembinaan ASN pada Perangkat Daerah
e. Pelaksanaan fungsi lain yang diberikan oleh Walikota terkait dengan tugas dan fungsinya.

2.9. Quality of Service (QoS)

Menurut Sofana (2017), *Network QoS* didefinisikan sebagai kinerja keseluruhan dari suatu *network*, yaitu kinerja yang dirasakan “secara riil” oleh pengguna *network* tersebut. Tujuan utama *QoS* adalah untuk menjamin aliran data bagi aplikasi hingga level tertentu, seperti tersedia cukup *bandwidth*, dapat mengendalikan *latency* dan *jitter*, dan mengurangi *data loss*.

QoS dapat diukur secara kuantitatif. Untuk mengukurnya, harus diketahui berbagai karakteristik network yang dapat mempengaruhi QoS, antara lain : *packet loss, delay, jitter, bandwidth* dapat dilihat pada Tabel 2.5. Karakteristik *network*

Tabel 2. 5. Karakteristik *Network*

Karakteristik network	Keterangan
Packet Loos	Nilai paket data yang hilang
Latency	Delay antara pengirim (*source*) dan penerima (*destination*).
Jitter	Variasi dari *delay/latency*
Bandwidth	Kecepatan *traffic* pada *network*.

Pada *computer network* (dan *packet-switched telecommunication networks*), *QoS* mengacu pada prioritas pemanfaatan *resource network*. Dengan *QoS* dapat ditentukan prioritas penggunaan *network* berdasarkan jenis aplikasi, *user*, aliran data.

QoS sangat penting untuk *transport traffic* yang memerlukan penanganan khusus. Saat ini *developer* telah membuat berbagai aplikasi yang dapat memanfaatkan komputer secara optimal, mulai dari aplikasi *web, email*, audio, video dan sebagainya. Berikut ini Tabel 2.6. Contoh aplikasi yang terkait dengan keempat karakteristik *network*

Tabel 2. 6. Contoh aplikasi

Aplikasi	***Packet Loos***	***Latency***	***Jitter***	***Bandwidth***
Email	*Low*	*Low*	*Low*	*Low*
File transfer	*Low*	*Low*	*Low*	*Medium*
Web access	*Low*	*Medium*	*Low*	*Medium*
Remote login	*Low*	*Medium*	*Medium*	*Low*
Audio on demand	*High*	*Low*	*High*	*Medium*
Video on demand	*High*	*Low*	*High*	*High*
Telephony	*High*	*High*	*High*	*Low*
Video conferencing	*High*	*High*	*High*	*High*

2.10. Desain *Top-down*

Menurut Oppenheimer (2011), Desain jaringan *top-down* adalah metodologi untuk merancang jaringan yang dimulai pada lapisan atas model referensi *OSI* sebelum pindah ke lapisan bawah. Metodologi *top-down* berfokus pada aplikasi, sesi, dan transportasi data sebelum pemilihan *router, switch*, dan media yang beroperasi di lapisan bawah.

Dalam metodologi *top-down* dapat dibedakan menjadi beberapa bagian antara lain

a. Bagian I: Mengidentifikasi Kebutuhan dan Tujuan Setda Salatiga

Bagian I mencakup tahap analisis persyaratan. Fase ini dimulai dengan mengidentifikasi bisnis tujuan dan persyaratan teknis. Mengklasifikasikan karakteristik jaringan yang ada, termasuk arsitektur dan kinerja segmen dan perangkat jaringan utama, mengikuti. Langkah terakhir dalam fase ini adalah menganalisis lalu lintas jaringan, termasuk arus dan beban lalu lintas, perilaku protokol, dan persyaratan kualitas layanan (*QoS*).

b. Bagian II: Desain Jaringan Logis

Selama fase desain jaringan logis, perancang jaringan mengembangkan *topologi* jaringan. Bergantung pada ukuran karakteristik jaringan dan lalu lintas, *topologi* dapat berkisar dari yang sederhana hingga kompleks, yang membutuhkan hierarki dan modularitas. Selama fase ini, perancang jaringan juga merancang model pengalamatan lapisan jaringan dan memilih protokol *switching* dan *routing*. Desain logis juga mencakup perencanaan keamanan, desain manajemen jaringan, dan penyelidikan awal di mana penyedia layanan dapat memenuhi persyaratan *WAN* dan *remote-access*.

c. Bagian III: Desain Jaringan Fisik

Selama fase desain fisik, teknologi dan produk spesifik yang mewujudkan desain logis dipilih. Desain jaringan fisik dimulai dengan pemilihan teknologi dan perangkat untuk jaringan kampus, termasuk pemasangan kabel, sakelar *Ethernet*, nirkabel jalur akses, jembatan nirkabel, dan *router* . Memilih teknologi dan perangkat untuk akses jarak jauh dan kebutuhan *WAN*. Juga, penyelidikan ke penyedia layanan, yang dimulai selama fase desain logis, harus diselesaikan selama fase ini.

d. Bagian IV: Menguji, Mengoptimalkan, dan Mendokumentasikan Desain Jaringan

Langkah terakhir dalam desain jaringan *top-down* adalah untuk menulis dan menerapkan rencana pengujian, membangun *prototipe*, mengoptimalkan desain jaringan, dan mendokumentasikan pekerjaan dengan proposal desain jaringan.

Jika hasil pengujian menunjukkan adanya masalah kinerja, selama fase ini harus memperbarui desain untuk menyertakan fitur optimisasi seperti pembentukan lalu lintas dan mekanisme antrian dan *switching router* lanjutan

2.11. Mikrotik

Menurut Sofana(2017), MikroTik pada mulanya adalah sebuah perusahaan kecil (kini sudah menjadi perusahaan besar) yang berkantor pusat di Riga Latvia, sebuah negara di Eropa. MikroTik mula-mula dibangun oleh John Trully dan Arnis Riekstins pada tahun 1995.

Sejarah MikroTik dimulai pada tahun 1996 di Moldova, yaitu saat John dan Arnis mulai menggabungkan sistem *Linux* dan *MS DOS* dengan teknologi *Wireless LAN (W-LAN) AERONET* yang berkecepatan sekitar 2Mbps. Kernel *Linux* yang digunakan pertama kali adalah Kernel versi 2.2.

a. Mikrotik RouterOS™

Mikrotik RouterOS™merupakan sistem operasi yang diperuntukan sebagai *network router*. Mikrotik RouterOS™sendiri adalah sisitem operasi dan perangkat lunak yang dapat membuat komputer biasa menjadi sebuah *router network* yang handal. Fitur-fitur yang disediakan oleh Mikrotik RouterOS™antara lain :

1) *Protokol TCP/IP (Layer3)*
   a) *Firewall* dan *NAT*
   b) *Static/Dynamic routing*
   c) *Hotspot*
   d) *Point to Point Tunneling Protocol*
   e) *DNS server*
   f) *Caching DNS client*
   g) *DHCP server*
   h) *Data Rate Management*
   i) *Simple tunnels*
   j) *Ipsec*
   k) *Web proxy*
   l) *Universal Client*

m) *VRRP*
n) *UpnP*
o) *NTP*
p) *Monitoring / Accounting*
q) *SNMP*
r) *M_3P*
s) *MNDP* dan lain sebagainya

2) *Protokol Layer 2*
a) *Wireless*
b) *Bridge*
c) *Virtual LAN*
d) *Synchronous*
e) *Asnchronous*
f) *ISDN*
g) *SDSL*

Mikrotik RouterOS™ didesain untuk memberikan kemudahan bagi penggunanya. Administrasinya bisa dilakukan melalui aplikasi Windows yang disebut WinBox.

b. Mikrotik RouterOS™

Mikrotik RouterOS™ merupakan sistem operasi berlisensi namun *file image* Mikrotik RouterOS™ bisa diunduh dari *website* resmi Mikrotik, www.mikrotik.com/download. *File image* ini merupakan versi *trial* yang hanya dapat digunakan dalam waktu 24 jam. Untuk dapat menggunakannya secara penuh, harus membeli lisensi. Satu lisensi hanya *valid* untuk satu buah *hardisk.*

Mikrotik RouterOS™ terdiri atas beberapa level, mulai dari level 0 hingga level 6 berikut penjelasansingkat masing-masing level

1) Level 0, merupakan lisensi versi *trial* dimana RouterOS dapat digunakan secara gratis selama 24 jam sejak RouterOS diinstal
2) Level 1, merupakam versi demo dan hanya dapat digunakan oleh 1 pengguna
3) Level 3, hanya untuk *client* dan hanya ada pada perangkat RouterBOARD
4) Level 4, dapat digunakan sebagai *router* dengan semua fitur umum sebuah

router, seperti *OSPF*, *BGP*, *RIP* dan juga untuk *wireless clientatau serial interface*

5) Level 5, mirip dengan level 4 namun jumlah pengguna lebih banyak
6) Level 6 tanpa batasan apa pun

c. Mikrotik Router

Mikrotik Router adalah - perangkat keras (*hardware*) *router* buatan Mikrotik yang menjalankan sistem RouterOS. Secara umum ada dua kelompok mikrotik *router*, yaitu:

1) *Integrated*, merupakan perangkat *router* yang lengkap dengan *casing* dan *power supply*
2) *RouterBOARD*, merupakan *motherboard* tanpa *power supply*, *interface* dan *casing*. *Router* jenis ini dapat modifikasi dan disesuaikan dengan kebutuhan pengguna.