BAB II

TINJAUAN UMUM

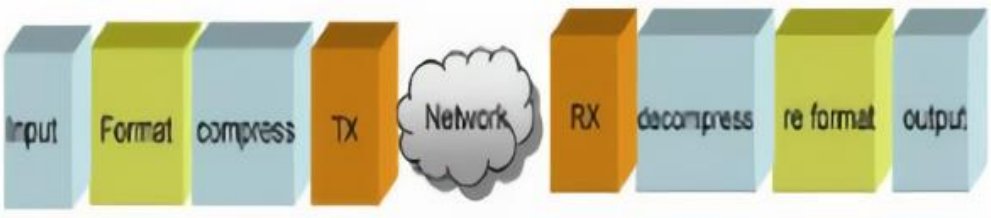
2.1 *Video*

Video adalah informasi yang berisi gambar dan suara serta memiliki ciri khas gambar bergerak dengan kecepatan tertentu atau *frame per second*[1]. Parameter video menentukan kualitas video, berdasarkan Adobe pada tahun 2014 terdapat 3 parameter video, yakni :

a) *Frame per Second* (FPS), adalah banyaknya *frame* yang dimainkan tiap detik. Nilai FPS adalah 20 hingga 30 fps.
b) Bitrate, adalah nilai pengukuran dari bit yang dikirimkan per waktu tertentu.
c) Resolution, adalah ukuran gambar yang ditampilkan pada layar.

2.2 *Video Conference*

Video conference merupakan suatu sistem yang dirancang guna memudahkan dua orang atau lebih berkomunikasi dalam jarak yang berbeda namun dengan waktu yang bersamaan. Video conference menggunakan telekomunikasi yang meliputi pelayanan data, voice, multimedia dan berupa video dan audio serta internet[4]. *Video conference* merupakan layanan komunikasi interaktif jarak jauh yang mampu mempertemukan dua orang atau lebih dengan memanfaatkan layanan internet *broadband.* Dimana layanan ini dapat mengirim dan menerima data yang berupa audio dan video secara bersamaan atau sering di sebut dengan teknik pengiriman dua arah. Konsep dasar dari *video conference* ini adalah menangkap data berupa suara dari mikrophone dan kamera lalu mengubahnya menjadi bit – bit data yang akan ditransmisikan[3].



Gambar 2.1 Proses Terjadinya *Video Conference* [3]

Pada *video conference* proses pengiriman dan penerimaan data bermula pada proses pengambilan gambar, menganalisa gambar, *compresing*, transmisi, *decoding*,dan terakhir *display*. Sebagai ilustrasi dapat dilihat pada Gambar 2.1. Untuk melakukan *video conference* terdapat dua jenis yaitu *video conference point to point* dan *video conference multipoint*. Dengan perbedaan teknik tersebut, tentunya berbeda juga kebutuhan *bandwidthnya*. Dimana penggunaan *bandwidth* pada *video conference multipoint* lebih besar dari pada layanan *video conference point to point*. Semakin banyaknya pengguna (*client*) maka beban trafik akan semakin besar juga[3].

Video conference menggunakan *webcam* sebagai data sumber yang akan dikirimkan. *Webcam* memiliki resolusi pengambilan gambar, resolusi antar satu *webcam* dengan *webcam* yang lain dapat bervariasi. Dahulu, *webcam* masih memiliki resolusi yang kecil, misalnya 160x120. Namun sekarang sudah ada *webcam* yang memiliki resolusi beberapa megapixel. Semakin besar ukuran resolusi, semakin besar pula jumlah data yang dikirimkan, sehingga *bandwidth* yang diperlukan juga semakin besar. Oleh karena itu, jarang sekali dilakukan *video conference* dengan ukuran resolusi yang besar. Umumnya ukuran resolusi yang digunakan untuk *video conference* adalah 320x240[9].

Video conference juga menggunakan sebuah *microphone* untuk input audio. Sama halnya dengan data video, terdapat faktor yang dapat mempengaruhi ukuran data yang dikirimkan, misalnya sampling rate (dalam satuan kHz) dan jumlah *channel*. Pada umumnya, ukuran data audio yang dikirimkan melalui streaming ini lebih kecil dibandingkan dengan data video. Sebuah data audio yang tidak dikompres menghasilkan data sebesar 5 *megabyte* per *channel* per menit. Tetapi, masih dimungkinkan jika input dari device ingin dikompres sehingga lebih menghemat *bandwidth* yang ada[9].

2.3 Router

Router merupakan sebuah perangkat keras yang digunakan untuk melewatkan IP dari suatu jaringan ke jaringan lainnya. Router berkemampuan melewatkan IP dari suatu jaringan ke jaringan lainnya yang mungkin memiliki lebih

dari satu jalur[6]. Router berada pada layer tiga (*network layer*) dalam OSI layer. Router juga merupakan sebuah perangkat jaringan komputer yang digunakan sebagai penghubung antar jaringan atau *network*. Router juga digunakan untuk meneruskan paket-paket data dari sebuah jaringan ke jaringan yang lain, baik dalam lingkup jaringan *Local Area Network* (LAN) maupun *Wide Area Network* (WAN). Router memiliki banyak modul yang dapat dipasang pada bagian belakang router sesuai dengan interface yang diinginkan seperti Ethernet, Fast Ethernet, Gigabit Ethernet, dan kabel serial. Konfigurasi router dilakukan dengan menggunakan IOS command[6].

2.3.1 Mikrotik *Router*

MikroTik dikenal luas sebagai router. *Router* merupakan perangkat jaringan yang digunakan untuk menghungkan beberapa jaringan (*Network*). Dalam jaringan yang lebih kompleks, router digunakan untuk memilahkan bagi paket data untuk mencapai komputer tujuan. Beberapa implementasi router yang paling sering digunakan adalah pembagian bandwith, pengaturan IP dan jalur, *security* berbasis *firewall* dan lain-lain.

Gambar 2.2 Router MikroTik[10]

MikroTik router merupakan suatu perangkat keras dalam jaringan komputer yang menggunakan sistem operasi berupa software MikroTik RouterOS dan diperuntukkan bagi network router. MikroTik Router OS adalah suatu sitem operasi

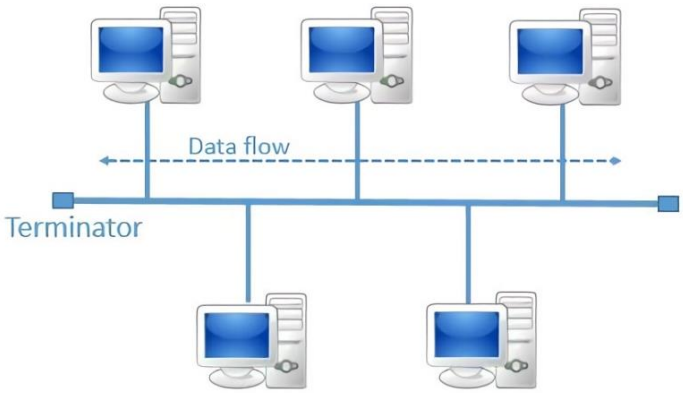
yang dibangun untuk network router. MikroTik Router OS didesain untuk memberikan kemudahan bagi pengguna[6]. MikroTik router memiliki beberapa fungsi yaitu *bandwidth management, stateful firewall, hotspot for plug and paly access, remote* WinBox GUI admin serta routing. Proses administrasi MikroTik router menggunakan Windows Application (WinBox)[8].

2.4 Topologi Jaringan Komputer

Topologi jaringan komputer merupakan cara untuk menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Cara yang saat ini banyak digunakan adalah *bus, token ring*, dan *star*. Dalam suatu jaringan komputer jenis topologi yang dipilih akan mempengaruhi kecepatan komunikasi. Untuk itu maka perlu dicermati kelebihan/keuntungan dan kekurangan/kerugian dari masing-masing topologi berdasarkan karakteristik yang dimilikinya[11].

2.4.1 Topologi *Bus*

Media penghantar untuk jenis topologi *bus* adalah kabel Koaksial. Topologi *bus* menggunakan metode *unicast, multicast* dan *broadcast*. *Unicast* adalah komunikasi antara satu pengirim dengan satu penerima di jaringan. *Multicast* adalah komunikasi antara satu pengirim dengan banyak penerima di jaringan. Sedangkan pada *broadcast*, setiap titik akan menerima dan menyimpan frame yang disalurkan/dihantarkan[11]. Karakteristik topologi bus disajikan pada Tabel 2.



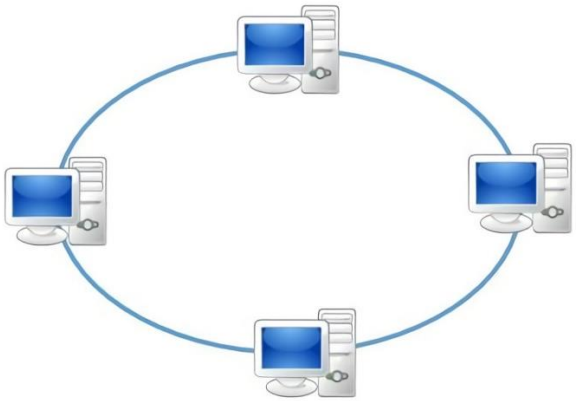
Gambar 2.3 Topologi *Bus*[12]

Tabel 2.1 Karakteristik Topologi *Bus*[11]

Keuntungan	Kerugian
a) Hemat kabel b) Layout kabel sederhana c) Mudah dikembangkan	a) Deteksi dan isolasi kesalahan sangat kecil b) Kepadatan lalu lintas c) Bila salah satu client rusak, maka jaringan tidak bisa berfungsi d) Diperlukan repeater untuk jarak jauh

2.4.2 Topologi *Ring*

Topologi token-ring (*ring*) menghubungkan komputer sehingga berbentuk *ring* (lingkaran). Setiap simpul mempunyai tingkatan yang sama. Jaringan akan disebut sebagai loop, data dikirimkan ke setiap simpul dan setiap informasi yang diterima simpul diperiksa alamatnya apakah data itu untuknya atau bukan[11]. Karakteristik topologi *ring* seperti disajikan pada Tabel 2.2.



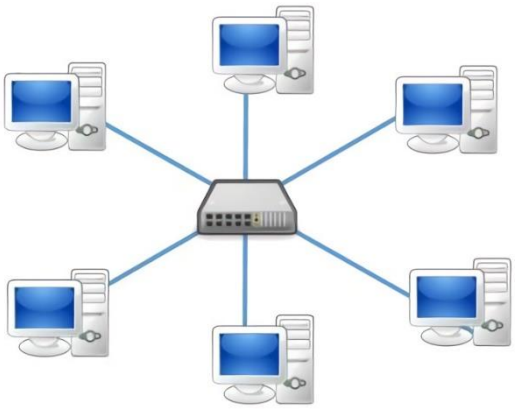
Gambar 2.4 Topologi *Ring*[12]

Tabel 2.2 Karakteristik Topologi *Ring*[11]

Keuntungan	Kerugian
a) Hemat kabel	a) Peka kesalahan b) Pengembangan jaringan lebih kaku

2.4.3 Topologi *Star*

Topologi *star* merupakan kontrol terpusat, semua *link* harus melewati pusat yang menyalurkan data tersebut ke semua *client* yang dipilihnya. *Client* pusat dinamakan stasiun primer atau server dan lainnya dinamakan stasiun sekunder atau *client* server. Setelah hubungan jaringan dimulai oleh server maka setiap *client* server sewaktu-waktu dapat menggunakan hubungan jaringan tersebut tanpa menunggu perintah dari server[11]. Karakteristik topologi *ring* seperti disajikan pada Tabel 2.3.



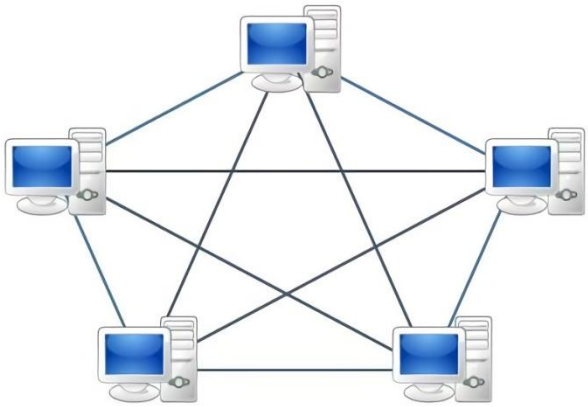
Gambar 2.5 Topologi *Star*[12]

Tabel 2.3 Karakteristik Topologi *Star*[11]

Keuntungan	Kerugian
a) Paling fleksibel b) Pemasangan/perubahan stasiun sangat mudah dan tidak mengganggu bagian jaringan lain c) Kontrol terpusat d) Kemudahan deteksi dan isolasi kesalahan/kerusakan e) Kemudahaan pengelolaan jaringan	a) Boros kabel b) Perlu penanganan khusus c) Kontrol terpusat (HUB/Switch) jadi elemen kritis

2.4.4 Topologi *Mesh*

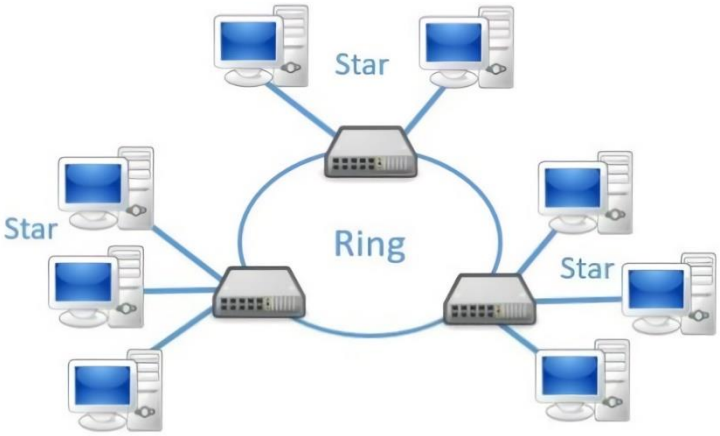
Topologi *mesh* dibangun dengan memasang banyak link pada setiap komputer. Hal ini dimungkinkan karena pada setiap komputer terdapat lebih dari satu NIC. Topologi ini secara teori memungkinkan akan tetapi tidak praktis dan biayanya cukup tinggi. Topologi Mesh memiliki tingkat *redundancy* yang tinggi[11].



Gambar 2.6 Topologi *Mesh*[12]

2.4.5 Topologi *Hybrid*

Topologi *hybrid* merupakan jaringan yang dibentuk dari berbagai topologi dan teknologi. Sebuah topologi *hybrid* memiliki semua karakterisitik dari topologi dasar yang terdapat dalam jaringan tersebut[11].



Gambar 2.7 Topologi *hybrid*[12]

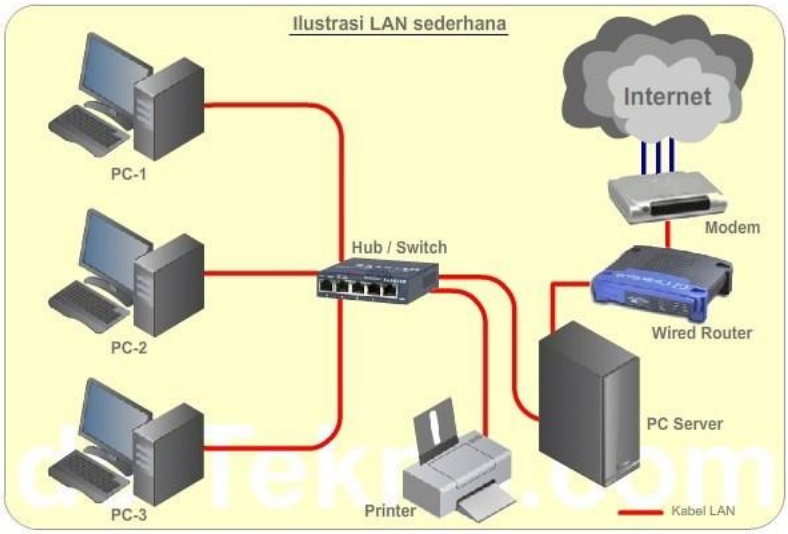
2.4.6 Topologi *Wireless*

Topologi *wireless* menggunakan gelombang radio untuk berkomunikasi dengan lainnya. Topologi *wireless* ini merupakan topologi yang sedang *trend* saat ini, karena mempunyai keunggulan lebih *mobile* dalam berkomunikasi. Topologi ini dapat berdiri sendiri dan secara umum banyak dipadukan dengan topologi dasar dalam aplikasinya[11].

2.5 *Local Area Network* (LAN) dan *Wireless Local Area Network* (WLAN)

2.5.1 *Local Area Network* (LAN)

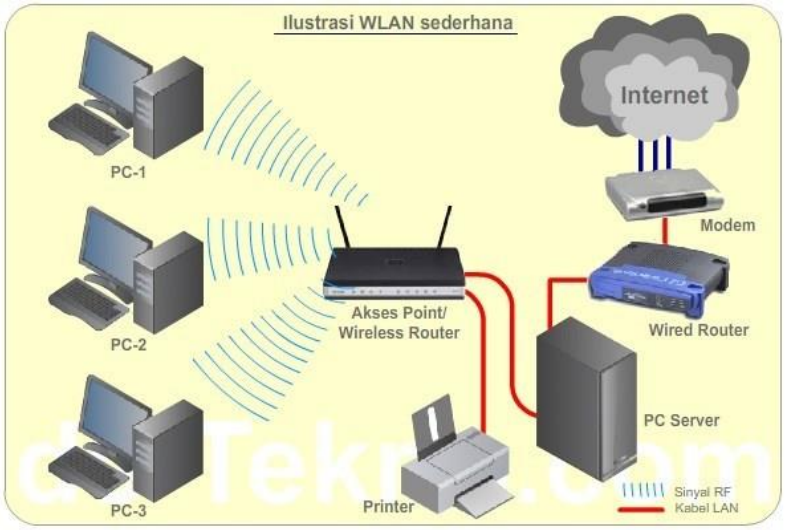
Local Area Network (LAN) merupakan seebuah jaringan yang menghubungkan antara komputer satu dengan komputer lainnya melalui sebuah Hub/Switch dengan menggunakan kabel LAN yang dikontrol oleh sebuah komputer server. Jaringan LAN juga dilengkapi router dan modem untuk koneksi ke jaringan internet dan dibagikan ke setiap komputer di dalam jaringan sehingga masing-masing komputer pun dapat mengakses internet dibawah kontrol komputer induk atau server. Struktur jaringan LAN sebenarnya sangat kompleks, namun ini sekedar gambaran sederhananya agar lebih mudah dipahami. Jaringan LAN ini banyak digunakan di kantor-kantor atau perusahaan, untuk saling bertukar data, kirim email diantara sesama karyawan di kantor atau perusahaan tersebut[13].



Gambar 2.8 Ilustrasi LAN Sederhana[13]

2.5.2 *Wireless Local Area Network* (WLAN)

Hampir sama dengan LAN, namun koneksi antar perangkat komputer di dalam jaringan tidak menggunakan kabel tapi menggunakan sinyal gelombang radio yang dipancarkan oleh sebuah *Access Point* (AP) sebagai pengganti Hub/Switch dalam jaringan LAN. Dan masing-masing komputer di dalam jaringan WLAN dilengkapi *Wireless Adapter* untuk bisa menerima sinyal radio yang dipancarkan oleh Akses Point. Wi-Fi adalah bentuk lain dari WLAN yang menggunakan teknologi jaringan *wireless* sesuai dengan standard 802.11 IEEE. Jadi, Wi-Fi = WLAN + standard 802.11[13].



Gambar 2.9 Ilustrasi WLAN Sederhana[13]

2.6 Internet

Internet merupakan jaringan komputer yang terhubung menggunakan standar sistem global Transmission Control Protocol/Internet Protocol (TCP/IP) sebagai protokol pertukaran paket data untuk melayani pengguna di seluruh dunia. Dengan internet, maka lalu lintas data dari seluruh belahan dunia dapat saling berbagi informasi yang diperlukan. Internet Protocol (IP) merupakan inti dari TCP/IP dan merupakan protokol terpenting dalam Internet *Layer*, dimana IP menyediakan pelayanan pengiriman paket pada jaringan TCP/IP yang dibangun. Teknologi internet ini menggunakan fasilitas layanan yang biasa kita sebut dengan *World Wide Web* (www)[14].

2.7 *Virtual Private Network* (VPN)

Virtual Private Network (VPN) merupakan teknologi dalam komunikasi yang dapat menghubungkan jaringan public ke jaringan local. Dengan begitu, suatu jaringan public tersebut bisa mendapatkan hal dan pengaturan yang sama dengan suatu jaringan local. Teknologi VPN menyediakan beberapa fungsi utama untuk penggunaannya. Fungsi-fungsi utama tersebut antara lain sebagai berikut[14]:

1. *Confidentially* (Kerahasiaan)
2. Data *Intergrity* (Keutuhan data)
3. *Origin Authentication* (Autentikasi sumber)
4. *Non-repudiation*
5. Kendali akses

Secara umum semua type tersebut memiliki fungsi yg sama. Yang membedakan adalah autentikasi dan enkripsi yg digunakan. Berikut tipe-tipe VPN[15]:

1. PPTP (*Point to Point Tunnel Protocol*)

   PPTP merupakan salah satu type VPN yang paling sederhana dalam konfigurasi. Selain itu juga fleksibel. Mayoritas *operating system* sudah support sebagai PPTP *Client*, baik *operating system* pada PC ataupun *gadget* seperti android. Komunikasi PPTP menggunakan protokol TCP port 1723, dan menggunakan IP Protocol 47/GRE untuk enkapsulasi paket datanya. Pada setting PPTP, kita bisa menentukan *network security protocol* yang digunakan untuk proses autentikasi PPTP pada MikroTik, seperti pap,chap,mschap dan mschap2. Kemudian setelah tunnel terbentuk, data yang ditransmisikan akan dienkripsi menggunakan Microsoft Point-to-Point Encryption (MPPE). Proses enskripsi biasanya akan membuat ukuran header paket yang ditransmisikan akan bertambah. Jika kita monitoring, *traffick* yang melewati tunnel PPTP akan mengalami *overhead* 7%.

2. L2TP (*Layer 2 Tunnel Protocol*)

   L2TP merupakan pengembangan dari PPTP ditambah L2F. *Network security Protocol* dan enkripsi yang digunakan untuk autentikasi sama dengan PPTP. Akan tetapi untuk melakukan komunikasi, L2TP

menggunakan UDP port 1701. Biasanya untuk keamaanan yang lebih baik, L2TP dikombinasikan dengan IPSec, menjadi L2TP/IPSec. Contohnya untuk *Operating system* Windows, secara default OS Windows menggunakan L2TP/IPSec. Akan tetapi, konsekuensinya tentu saja konfigurasi yang harus dilakukan tidak se-simple PPTP. Sisi client pun harus sudah support IPSec ketika menerapkan L2TP/IPSec. Dari segi enkripsi, tentu enkripsi pada L2TP/IPSec memiliki tingkat sekuritas lebih tinggi daripada PPTP yg menggunakan MPPE. *Traffick* yang melewati tunnel L2TP akan mengalami *overhead* 12%.

3. SSTP (*Secure Socket Tunneling Protocol*)

   Untuk membangun vpn dengan metode SSTP diperlukan sertifikat SSL di masing-masing perangkat, kecuali keduanya menggunakan RouterOS. Komunikasi SSTP menggunakan TCP port 443 (SSL), sama hal nya seperti *website* yang *secure* (https). Anda harus memastikan *clock* sudah sesuai dengan waktu *real* jika menggunakan *certificate*. Manyamakan waktu router dengan real time bisa dengan fitur NTP Client. Sayangnya belum semua OS *Support* VPN dengan metode SSTP. *Traffick* yang melewati tunnel SSTP akan mengalami *overhead* 12%.

4. OpenVPN

   VPN ini Biasa digunakan ketika dibutuhkan keamanan data yg tinggi. Secara *default*, OpenVPN menggunakan UDP port 1194 dan dibutuhkan *certificate* pada masing-masing perangkat untuk bisa terkoneksi. Untuk *client compatibility*, OpenVPN bisa dibangun hampir pada semua *Operating System* dengan bantuan aplikasi pihak ketiga. OpenVPN menggunakan algoritma sha1 dan md5 untuk proses autentikasi, dan menggunakan beberapa *chiper* yaitu blowfish128, aes128, aes192 dan aes256. Trafik yang melewati tunnel OpenVPN akan mengalami *overhead* 16%.

2.8 *Internet Protocol Address* (Alamat IP)

Internet Protocol Address atau alamat IP merupakan kode pengenal komputer pada jaringan dan merupakan kode vital dalam dunia internet. Alamat IP dapat dikatakan sebagai identitas dari pemakai internet, sehingga antara satu alamat dengan alamat lainnya tidak boleh sama. *Internet Protocol* (IP) pada awalnya dirancang untuk memfasilitasi hubungan antara beberapa organisasi yang tergabung dalam departemen pertahanan amerika yaitu *Advanced Research Project Agency* (ARPA). Sebelum terciptanya internet protocol, jaringan memiliki peralatan dan protocol tersendiri yang digunakan untuk saling berhubungan. Kemudian dibuatlah suatu protocol yang dapat dapat digunakan secara umum untuk menyatukan berbagai perbedaan dalam penggunaan perangkat yang terhubung didalam jaringan. Protocol tersebutlah yang sampai saat ini masih mendominasi dalam pemakaiannya oleh masyarakat banyak yaitu *Internet Protocol version* 4 (IPv4)[16].

IP *Address* dibagi atas tiga bagian diantaranya[17]:

1. Berdasarkan cakupan penggunaannya dalam jaringan komputer sehari-hari dalam jaringan lokal maupun jaringan internet publik, IP *Address* dibagi menjadi dua jenis, yaitu:
   a. IP *Address Public*

      IP *Address public* adalah IP *Address* yang dimiliki oleh setiap komputer atau perangkat yang terhubung lainnya dan digunakan pada jaringan internet (publik). Kepemilikannya diatur oleh vendor-vendor terkait yang menyediakannya, contoh Internet Service Provider.

   b. IP *Address Private*

      IP *Address private* adalah IP *Address* yang digunakan oleh komputer atau perangkat yang terhubung lainnya dan umumnya digunakan oleh jaringan berskala lokal atau *Local Area Network* (LAN). Hal ini memungkinkan penggunaan alamat yang sama dengan syarat, yakni jaringan satu dan jaringan lainnya tidak saling terhubung dalam jaringan lokal.
2. Berdasarkan dari bagaimana pengguna melakukan konfigurasi untuk memperoleh IP *Address*, IP *Address* dibagi menjadi dua jenis, yaitu:

a. IP *Address* Dinamis (*Dynamic* IP *Address*)

IP *Address* jenis ini adalah pemberian secara otomatis dalam jaringan *public* maupun *private* yang akan diberikan kepada komputer atau perangkat lainnya yang saling terhubung ke dalam jaringan komputer secara otomatis dan akan selalu berubah setiap saat (dinamis).

Untuk pemberiannya sendiri diberikan oleh sebuah perangkat, aplikasi sekaligus *protocol* di dalam jaringan komputer yang bernama *Dynamic Host Konfiguration Protocol* (DHCP). Sedangkan yang bertindak mengaktifkan DHCP adalah komputer atau perangkat yang dijadikan sebagai DHCP Server.

b. IP *Address* Statis

IP *Address* jenis ini adalah pemberian IP *Address* kepada komputer atau perangkat lainnya yang terhubung ke dalam jaringan komputer secara manual. Dalam hal ini, pengguna harus mengetahui pembagian kelas IP *Address*, Subnet, *Gateway*, dan DNS dalam sebuah jaringan.

3. Berdasarkan dari daya tampung komputer atau perangkat lainnya yang terhubung ke dalam jaringan komputer, IP *Address* dibagi menjadi dua jenis, yaitu:

a. IPv4 (IP *Address* Versi 4)

IP versi 4 atau IPv4 terdiri dari 32-bit dan bisa menampung lebih dari 4.294.967.296 host di seluruh dunia. Sebagai contoh adalah 172.146.80.100. Apabila *host* di seluruh dunia melebihi angka 4.294.967.296 maka dibuatlah IPv6. Angka besar ini untuk teknologi yang maju, tidak relevan untuk menampung alamat semua komputer dan perangkat yang saling terhubung. Untuk mengatasi keterbatasan ini salah satu caranya adalah menggunakan *Network Address Translation* (NAT). NAT merupakan sebuah cara untuk membagi, mengubah, dan memodifikasi pemetaan dari sebuah IP *Address*. Alamat IP (IPv4) pada awalnya adalah sederet bilangan biner sepanjang 32 bit yang dipakai untuk mengidentifikasikan host pada jaringan. Alamat IP ini diberikan secara unik pada masing-masing komputer/host yang terhubung ke internet.

Prinsip kerjanya adalah *packet* yang membawa data dimuati alamat IP dari komputer pengirim data kepada alamat IP pada komputer yang akan dituju, kemudian data tersebut dikirim ke jaringan. *Packet* ini kemudian dikirim dari *router* ke *router* dengan berpedoman pada alamat IP tersebut menuju ke komputer yang dituju. Seluruh komputer/host yang tersambung ke internet, dibedakan hanya berdasarkan alamat IP ini, oleh karena itu tidak boleh terjadi duplikasi pada alamat IP untuk setiap komputer yang terhubung ke jaringan internet. Alamat-alamat IP panjangnya 32 bit dan dibagi menjadi dua identifikasi sebagai berikut[16]:

1) Bagian identifikasi net ID menunjukkan identitas jaringan komputer tempat host-host (komputer) dihubungkan.
2) Bagian identifikasi host ID memberikan suatu pengenal unik pada setiap host (komputer) pada suatu jaringan komputer.

b. IPv6 (IP *Address* Versi 6)

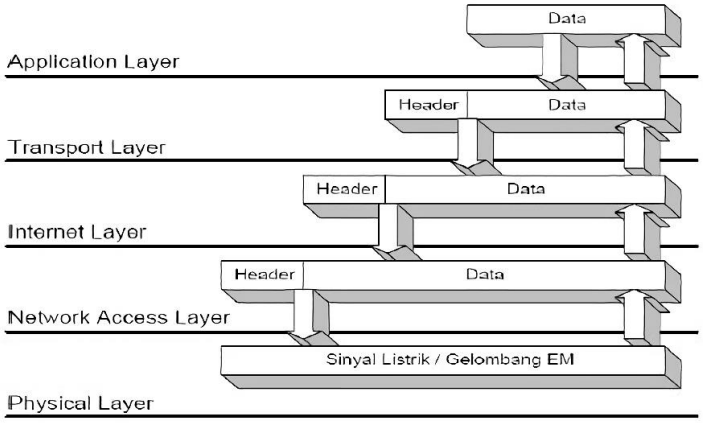
IPv6 diciptakan untuk menjawab kekhawatiran akan kemampuan IPv4 yang hanya menggunakan 32 bit untuk menampung IP *Address* di seluruh dunia. Semakin banyaknya pengguna jaringan internet dari hari ke hari di seluruh dunia, IPv4 dinilai suatu saat akan mencapai batas maksimum. Oleh karena itu, IPv6 versi 128 bit diciptakan. Kemampuan yang memang jauh lebih besar, dinilai akan mampu menyediakan IP *Address* pada seluruh pengguna jaringan internet di seluruh dunia.

IP versi 6 atau IPv6 ini terdiri dari 128 bit. IP ini 4 kali dari IPv4 namun jumlah *host* yang bisa ditampung bukanlah 4 kali dari 4.294.967.296 melainkan 4.294.967.296 pangkat 4. Jadi hasilnya 340.282.366.920.938.463.463.374.607.431.768.211.456.

2.9 *Transmission Control Protocol/Internet Protocol* (TCP/IP)

Transmission Control Protocol/Internet Protocol (TCP/IP) adalah suatu *protocol suite* yang digunakan untuk mengirim data antar komputer di dalam jaringan tanpa batasan perangkat keras maupun perangkat lunak. Protokol ini biasa digunakan untuk pengiriman data, informasi maupun kendali di dalam jaringan

komputer. TCP/IP hanya terdiri atas 5 lapisan (*layer*), yang mana tiap lapisan mengerjakan apa yang menjadi tugasnya tanpa terkait dengan tugas lapisan yang lain[18]. Gambaran lapisan pada TCP/IP dapat dilihat pada gambar 2.5.



Gambar 2.10 Proses Komunikasi Data Antar Lapisan TCP/IP[18]

Fungsi tiap lapisan pada TCP/IP dapat dijelaskan sebagai berikut[18]:

1. *Physical (hardware)*

   Lapisan ini merupakan lapisan terbawah dalam TCP/IP. Lapisan ini mendefinisikan besaran fisik suatu media komunikasi seperti: tegangan, arus maupun gelombang radio. Bentuknya dapat bervariasi tergantung pada media jaringan dan bersifat fleksibel sehingga dapat mengintegrasikan jaringan dengan berbagai media fisik yang berbeda.

2. *Network*

   Lapisan ini bertugas mengatur penyaluran data yang akan dikirimkan pada media fisik. Lapisan ini menjaga reliabilitas data yang akan dikirimkan. Pada lapisan ini, dilakukan deteksi dan koreksi kesalahan pada tingkat bit.

3. Internet

   Lapisan ini mendefinisikan bagaimana dua pihak dapat berhubungan walaupun berada pada jaringan yang berbeda. Pada jaringan internet yang terdiri atas puluhan juta host dan ratusan ribu jaringan lokal, lapisan ini bertugas untuk menjamin agar suatu paket yang dikirimkan dapat menenemukan tujuannya. Lapisan ini memiliki peranan penting, terutama

dalam mewujudkan internet *working* yang meliputi wilayah yang luas (*world wide internet*). Beberapa tugas penting pada lapisan ini adalah sebagai berikut:

a) *Addressing*, yaitu melengkapi tiap data dari alamat internet dari tujuan, yang dikenal dengan nama *Internet Protocol Address*. Oleh karena pengalamatan berada pada level ini, maka jaringan TCP/IP tidak tergantung pada jenis media maupun komputer yang digunakan.

b) *Routing*, yaitu menentukan ke mana data dikirim agar mencapai tujuannya. Fungsi ini merupakan fungsi terpenting dalam Internet Protocol. Sebagai protokol yang bersifat *connectionless*, proses *routing* sepenuhnya ditentukan oleh jaringan. Pengirim tidak memiliki kendali terhadap paket yang dikirimkan untuk bisa mencapai tujuannya. Router-router di dalam jaringan yang sangat menentukan dalam penyampaian data dari pengirim ke penerima.

4. Transport/Network

Lapisan ini menjamin reliabilitas data dikirim antara pengirim dan penerima pada tingkat segmen. Lapisan ini menjamin bahwa data yang diterima pada penerima adalah sama dengan data yang dikirimkan oleh pengirim. Pada lapisan ini, terdapat 2 protokol yang sering digunakan, yaitu:

a) *User Datagram Protocol* (UDP), protokol ini tidak menyediakan layanan pemeriksaan data dan bersifat *connectionless*. Seringkali digunakan sebagai *protocol transport* untuk data yang sensitif terhadap delay seperti video conference maupun untuk aplikasi *database* yang bersifat *query*.

b) *Transport Control Protocol* (TCP), protocol ini menyediakan layanan pemerikasaan data dan bersifat *connection oriented*. TCP digunakan untuk pengiriman data yang menuntut keandalan.

c) *Flow Control*, pengiriman data yang telah dipecah menjadi paket-paket tersebut harus diatur sedemikian rupa agar pengirim tidak sampai mengirimkan data dengan kecepatan yang melebihi kemampuan penerima dalam menerima data.

d) *Error Detection*, data dilengkapi dengan informasi yang dapat digunakan untuk memeriksa apakah data yang dikirimkan bebas dari kesalahan. Bila ditemukan kesalahan, data akan diabaikan dan pengirim akan mengirimkan ulang data tersebut. Hal ini dapat membuat performa jaringan menurun karena menimbulkan *delay*.

5. *Application*

Lapisan ini merupakan lapisan terakhir dalam arsitektur TCP/IP yang berfungsi mendefinisikan aplikasi yang dijalankan pada jaringan. Oleh karena itu terdapat banyak protokol pada lapisan ini sesuai dengan banyaknya aplikasi yang dapat dijalankan.

2.10 Wireshark

Wireshark merupakan salah satu *tools* atau aplikasi "*Network Analyzer*" atau penganalisa jaringan. Penganalisaan kinerja jaringan itu dapat melingkupi berbagai hal, mulai dari proses menangkap paket-paket data atau informasi yang berlalu-lalang dalam jaringan, sampai pada digunakan pula untuk *sniffing* (memperoleh informasi penting seperti *password email*, dll). *Wireshark* sendiri merupakan *free tools* untuk *Network Analyzer* yang ada saat ini. Dan tampilan dari wireshark ini sendiri terbilang sangat bersahabat dengan *user* karena menggunakan tampilan grafis atau *Graphical User Interface* (GUI)[19].

2.11 OpenMeetings

OpenMeetings adalah perangkat lunak yang digunakan untuk presentasi, pelatihan online, konferensi web, menggambar papan tulis kolaboratif dan mengedit dokumen, dan berbagi desktop pengguna. *Open Meetings* sistem *virtual* di mana masing-masing anggota pengguna tidak harus bertatap muka dalam satu ruangan tetapi dapat digantikan dengan teknologi *streaming* berbasis web dengan memanfaatkan jaringan internet/intranet.

OpenMeetings menggunakan fungsi *Application Programming Interface* atau API media server, yaitu *software* yang mengizinkan dua aplikasi terhubung satu sama lain sebagai remoting dan menggunakan Red5 atau Kurento sebagai

server streaming yang berbasis Java yang mendukung *streaming audio* ataupun *video*[20].

2.12 *Quality of Service*

Qulaity of Service (QoS) adalah salah satu metode yang digunakan sebagai pengukuran kinerja suatu jaringan. QoS digunakan untuk mengetahui karakteristik dan sifat dari suatu layanan[21]. QoS juga diartikasn sebagai kemampuan suatu jaringan untuk menyediakan layanan yang baik dengan menyediakan bandwidth, mengatasi jitter dan delay. Parameter QoS adalah *throughput, packet loss, latency* atau *delay* dan *jitter*[22].

QoS didesain untuk membantu *end user (client)* menjadi lebih produktif dengan memastikan *user* mendapatkan performansi yang handal dari aplikasi-aplikasi berbasis jaringan. QoS mengacu pada kemampuan jaringan untuk menyediakan layanan yang lebih baik pada trafik jaringan tertentu melalui teknologi yang berbeda-beda. Tujuan QoS yaitu untuk memenuhi kebutuhan-kebutuhan layanan yang berbeda namun menggunakan infrastruktur yang sama[23]. Adapun fungsi-fungsi dari QoS adalah sebagai berikut[23]:

1. Pengkelasan paket untuk menyediakan pelayanan yang berbeda-beda untuk kelas paket yang berbeda-beda.
2. Penanganan kongesti untuk memenuhi dan menangani kebutuhan layanan yang berbeda- beda.
3. Pengendalian lalu lintas paket untuk membatasi dan mengendalikan pengiriman paket- paket data.
4. Pensinyalan untuk mengendalikan fungsi-fungsi perangkat yang mendukung komunikasi di dalam jaringan IP.

Tabel 2.4 Indeks Parameter QoS[24]

Nilai	Persentase (%)	Indeks
3,8 – 4	95 – 100	Sangat Memuaskan
3 – 3,79	75 – 94,75	Memuaskan
2 – 2,99	50 – 74,75	Sedang
1 – 1,99	25 – 49, 75	Buruk

Untuk menghitung nilai indeks parameter QoS persamaan yang digunakan yaitu sebagai berikut[25]:

$$Nilai = \frac{Jumlah\ Indeks}{Rata{-}Rata\ Indeks} \quad (2.1)$$

Sedangkan untuk menghitung nilai persentase parameter QoS persamaan yang digunakan yaitu sebagai berikut[25]:

$$Persentase\ (\%) = \frac{Jumlah\ Indeks}{Jumlah\ Keseluruhan\ Indeks} \quad (2.2)$$

2.12.1 Parameter QoS

QoS terdiri dari beberapa parameter, diantaranya:

1. *Throughput*

   Troughput adalah kecepatan (*rate*) transfer data data yang diukur dalam satuan bps (*bit per second*). *Throughput* merupakan jumlah total kedatangan paket yang sukses dan diamati pada tujuan dalam interval waktu tertentu dibagi dengan durasi interval waktu tersebut[21].

   Perhitungan *throughput* dapat dicari menggunakan rumus sebagai berikut[24]:

$$\text{Throughput} = \frac{\text{Packet data yang diterima}}{\text{Lama pengamatan}} \quad (2.3)$$

   Tabel kategori *throughput* yang didapatkan berdasarkan standar TIPHON, antara lain sebagai berikut:

Tabel 2.5 Kategori Nilai *Throughput*[24]

Kategori	Troughput (bps)	Indeks
Sangat Bagus	100	4
Bagus	75	3
Sedang	50	2
Jelek	<25	1

Sumber: TIPHON

2. *Packet Loss*

Packet Loss menggambarkan suatu kondisi jumlah total packet yang hilang dapat terjadi karena *collision* dan *congestion* pada suatu jaringan. Hal ini berpengaruh pada semua aplikasi karena *retransmisi* akan mengurangi efisiensi jaringan secara keseluruhan meskipun jumlah *bandwidth* cukup tersedia untuk aplikasi-aplikasi tersebut. Umumnya perangkat jaringan memiliki *buffer* untuk menampung data yang diterima. Jika terjadi kongesti yang cukup lama, *buffer* akan penuh, dan data baru tidak akan diterima[21].

Perhitungan *packet loss* dapat dicari menggunakan rumus sebagai berikut[24]:

$$\text{Packet Loss} = \frac{\text{Packet data yang dikirim} - \text{Packet data yang diterima}}{\text{Packet data yang dikirim}} \text{x}100\% \quad (2.4)$$

Packet data yang diterima=Packet data yang dikirim – Packet data yang hilang

Packet loss versi *Telecommunications and Internet Protocol Harmonization Over Networks* (TIPHON) dikelompokkan menjadi empat kategori seperti terlihat pada Tabel 2.6.

Tabel 2.6 Kategori Nilai *Packet Loss*[24]

Kategori	Packet Loss (%)	Indeks
Sangat Bagus	0	4
Bagus	3	3
Sedang	15	2
Jelek	25	1

Sumber: TIPHON

3. *Delay*

Delay adalah waktu yang dibutuhkan oleh data untuk menempuh suatu jarak dari asal ke tujuan. *Delay* dapat dipengaruhi oleh beberapa factor diantaranya jarak, media fisik, congesti atau waktu proses yang lama[21].

Perhitungan *delay* dapat dicari menggunakan rumus sebagai berikut[24]:

$$\text{Delay} = \frac{\text{Total Delay}}{\text{Packet packet yang diterima}} \quad (2.5)$$

Delay versi *Telecommunications and Internet Protocol Harmonization Over Networks* (TIPHON) dikelompokkan menjadi empat kategori seperti terlihat pada Tabel 2.7.

Tabel 2.7 Kategori Nilai *Delay*[24]

Kategori	Delay (ms)	Indeks
Sangat Bagus	<150	4
Bagus	150 s/d 300	3
Sedang	300 s.d 450	2
Jelek	>450	1

Sumber: TIPHON

4. *Jitter*

Jitter terjadi diakibatkan oleh variasi-variasi dalam panjang suatu antrian dalam waktu pengolahan data dan juga dalam waktu penghimpunan paket-paket di akhir perjalanan *jitter*. *Jitter* juga disebut variasi *delay* yang menunjukkan jumlah variasi delay pada transmisi data di jaringan[21].

Perhitungan *jitter* dapat dicari menggunakan rumus sebagai berikut[24]:

$$\text{Jitter} = \frac{\text{Total variasi delay}}{(\text{Total packet} - 1)} \quad (2.6)$$

Kategori kinerja jaringan berbasis IP dalam *jitter* versi *Telecommunications and Internet Protocol Harmonization Over Networks* (TIPHON) mengelompokkan menjadi empat kategori penurunan kinerja jaringan berdasarkan nilai *Jitter* seperti terlihat pada Tabel 2.8.

Tabel 2.8 Kategori Nilai *Jitter*[24]

Kategori	Delay (ms)	Indeks
Sangat Bagus	<150	4
Bagus	150 s/d 300	3
Sedang	300 s.d 450	2
Jelek	>450	1

Sumber: TIPHON

2.12.2 Faktor Pengaruh Penurunan QoS

Nilai QoS dapat menurun dikarenakan beberapa faktor pengaruh. Faktor-faktor yang mempengaruhi penurunan QoS atau faktor-faktor pengganggu jaringan tersebut diantaranya:

1. Redaman

   Yaitu jatuhnya kuat sinyal karena pertambahan jarak pada media transmisi. Setiap media transmisi memiliki redaman yang berbeda-beda, tergantung dari bahan yang digunakan. Untuk mengatasi hal ini, perlu digunakan repeater sebagai bahan penguat sinyal. Pada daerah frekuensi tinggi biasanya mengalami redaman lebih tinggi dibandingkan pada daerah frekuensi rendah.

2. Distorsi

   Yaitu fenomena yang disebabkan bervariasinya kecepatan propagasi karena perbedaan *bandwidth*. Untuk itu, dalam komunikasi dibutuhkan bandwidth transmisi yang memadai dalam mengakomodasi adanya spectrum sinyal. Dianjurkan digunakan pemakaian *bandwidth* yang seragam, sehingga distorsi dapat dikurangi.

3. Noise

   Yaitu sinyal gangguan yang berbahaya, karena jika terlalu besar akan dapat mengubah data asli yang dikirimkan.

2.13 *Black Box Testing*

Black box testing atau yang sering dikenal dengan sebutan pengujian fungsional[26], merupakan pengujian yang didasarkan pada detail seperti tampilan, fungsi-fungsi yang ada, dan kesesuaian alur fungsi dengan bisnis proses yang diinginkan oleh *customer*. *Black box testing* ini lebih menguji ke tampilan luar (*interface*) dari suatu aplikasi agar mudah digunakan oleh *client*. Pengujian ini tidak melihat dan menguji *souce code* program. *Black box testing* bekerja dengan mengabaikan struktur *control* sehingga perhatiannya hanya terfokus pada informasi domain[27]. Pengujian ini dilakukan untuk meyakinkan semua input diterima dengan tepat, dan output yang dihasilkan juga tepat dan berjalan dengan baik. Dengan kata lain, metode pengujian *black box* adalah untuk mengetes hubungan antar program dalam sebuah sistem. Keuntungan dan kekurangan pada *black box testing* dapat dilihat pada tabel 2.8[28].

Tabel 2.9 Kelebihan dan Kelemahan *Black Box Testing*[28]

Kelebihan	**Kelemahan**
Perincian aplikasi dapat ditentukan di awal, dan pengujian dilakukan berdasarkan perincian spesifikasi tersebut.	Apabila keperluan perangkat lunak yang akan dikembangkan tidak begitu jelas, pembuatan dokumentasi yang tepat akan sedikit sulit.
Dapat dipakai untuk menilai konsistensi suatu aplikasi, dan tidak perlu melihat kode program secara detil.	Pengguna akan kurang merasa yakin dengan perangkat lunak yang diuji apakah lolos dalam standar pengujian.

Berikut beberapa teknik pada *black box testing* antara lain[27]:

1. *Equivalence Partitioning*

   Cara kerja teknik ini adalah dengan melakukan *partition* atau pembagian menjadi beberapa partisi dari *input* data.

2. *Boundary Value Analysis*

   Teknik ini lebih fokus kepada *boundary*, dimana adakah error dari luar atau sisi dalam *software*, minimum, maupun maximum nilai dari error yang didapat.

3. *Fuzzing*

   Fuzz merupakan teknik untuk mencari *bug*/gangguan dari *software* dengan menggunakan injeksi data yang terbilang cacat ataupun sesi semi-otomatis.

4. *Cause-Effect Graph*

   Ini adalah teknik *testing* dimana menggunakan *graphic* sebagai pacuannya. Dimana dalam grafik ini menggambarkan relasi diantara efek dan penyebab dari error tersebut.

5. *Orthogonal Array Testing*

   Dapat digunakan jika input domain yang relatif terbilang kecil ukurannya, tetapi cukup berat untuk digunakan dalam skala besar.

6. *All Pair Testing*

   Dalam teknik ini, semua pasangan dari *test case* di desain sedemikian rupa agar dapat di eksekusi semua kemungkinan kombinasi diskrit dari seluruh pasangan berdasar input parameternya. Tujuannya *testing* ini adalah memiliki pasangan *test case* yang mencakup semua pasangan tersebut.

7. *State Transition*

   Testing ini berguna untuk melakukan pengetesan terhadap kondisi dari mesin dan navigasi dalam bentuk grafik.

2.14 Penelitian Terdahulu

Tabel 2.10 Penelitian Terdahulu

No.	Judul	*Keywords*	Penulis	Tahun	Kelebihan	Kekurangan
1.	Perancangan Sistem Informasi *Video Conference*	*Meeting*, UML, *Video Conferenc e*	Ferina Ferdianti, Lia Ambarwati, Melisa	2012	Rancangan sistem *video conference* menyediakan fitur-fitur	Koneksi internet yang dibutuhkan harus berskala besar.

	Untuk Mendukung Rapat		Chatrine Kamu, dkk		untuk mendukung rapat misalnya berbagi file, media presentasi dan penyimpanan video	
2.	Implementasi OpenMeetings Menggunakan Raspberry PI Sebagai Server	Implementasi, , Raspberry PI, *Conference*, Web	Nur Afif	2017	Menu-menu yang ditampilkan pada *OpenMeetings* yang telah dibangun sangat lengkap. *User* yang tergabung dalam *video conference* terdata dengan *detail*.	Tidak menyediakan fitur-fitur untuk mendukung *video conference* misalnya berbagi file, media presentasi dan penyimpanan video
3.	Perancangan Dan Implementasi Hotspot Cerdas Berbasis Mikrotik OS Dan Web Server Mini PC Raspberry PI	*Router OS*, Mikrotik, *Firewall, Otentifikasi User, Managemen User*, Web server, Raspberry pi	Tria Aprilianto, Samsul Arifin	2018	Arsitektur jaringan yang dibangun cukup lengkap dan mudah dipahami	Belum ada penambahan sistem *e-learning* dalam jaringan lokal
4.	Analisis Kualitas Layanan QoS *video conference* pada Jaringan 4G *LTE* dengan menggunakan *Codec* H.264	*Codec H.264, lte, multipoint, QoS, video conference*	Anggar Wati	2018	Dalam penyampaian analisa dilakukan sangat detail sehingga mudah dalam dipahami.	Pengetesan jaringan hanya dilakukan dengan menggunakan empat provider, tidak dilakukan dengan menggunakan

						jaringan WLAN
5.	*Quality Of Service* (QoS) Layanan *video conference* Pada Jaringan *High Speed Packet Access* (HSPA) Menggunakan Emulator *Graphical Network simulator* (GNS) 3	*Video conference , Quality Of Service (QoS),* GNS3	Reno Muktiaji Herdiansyah	2013	Dalam penulisan hasil data, perhitungan dan analisa dilakukan sangat detail sehingga mudah dalam memahaminya.	Kualitas layanan *video conference* memiliki perbedaan untuk hasil pengamatan menggunakan GNS3. Perbedaan Hasil pengamatan terjadi karena perbedaan karakteristik *switching*, jumlah node dan rute data.