BAB 2
DASAR TEORI

2.1 KAJIAN PUSTAKA

Dalam penelitian yang dilakukan oleh Mudhoep, dkk [3] tahun 2021 dibahas mengenai perbandingan tiga protokol redundansi, yaitu VRRP, HSRP, dan GLBP, dengan kombinasi masing-masing menggunakan protokol *routing* OSPF dan BGP. Dalam penelitian ini, hanya digunakan QoS berupa *throughput*, *delay*, dan *packet loss*. Hasil penelitian menunjukkan bahwa metode kinerja VRRP memiliki rata-rata indeks yang lebih baik yaitu 3,90 daripada HSRP dan GLBP yang hanya sebesar 3,88. Sedangkan pada indeks QoS protokol *routing*, *routing* OSPF memiliki rata-rata indeks lebih baik yaitu 3,96 dibandingkan dengan BGP yang hanya sebesar 3,8. Selain itu, hasil pada parameter *packet loss* dan *delay* yaitu sebesar 0,017% dan 9,91 ms, menunjukkan hasil yang lebih baik dibandingkan dengan protokol BGP.

Penelitian Michael, dkk [4]tahun 2018 meneliti mengenai protokol redudansi VRRP menggunakan protokol *routing* OSPF menggunakan OS Mikrotik, dimana protokol redudansi VRRP memiliki kehilangan data yang kecil sebesar 3.8% sedangkan ketika tidak menggunakan VRRP memiliki kehilangan data yang besar yaitu 25.0% dan penggunaan tanpa VRRP dan menggunakan VRRP tidak berpengaruh pada *throughtput* dan *bandwitdh*.

Penelitian Dharma, dkk [5] meneliti terkait protokol *network* redudansi yang ada seperti VRRP, GLBP dan HSRP pada layanan video *streaming*. Setiap *router* protokol redundansi VRRP, HSRP dan GLBP diberikan nilai prioritas tertinggi secara bergantian pada *router* R2, R3, dan R4 sebesar 160. Sisanya yang akan menjadi *router backup* memiliki nilai prioritas yang lebih kecil sebesar 140 dan 120. hasil pengujian waktu perpindahan *link* serta kualitas layanan video *streaming* dengan tiga skenario simulasi kondisi jaringan normal, *down* dan *recovery*. Didapatkan bahwa protokol redundansi yang memiliki kinerja lebih baik pada layanan video *streaming* adalah GLBP. Kemudian disusul oleh VRRP dan HSRP. Hal ini dikarenakan pada GLBP memiliki fitur *load balancing*. Sehingga dengan fitur tersebut dapat memaksimalkan kinerja dalam proses transmisi

jaringan. Sementara terbaik kedua dari VRRP karena memiliki waktu *hello* dan *hold time* yang lebih cepat jika dibandingkan dengan HSRP.

Penelitian Shahriar dan Fan [6] tahun 2020 melakukan penelitian tentang analisis dari FHRP di jaringan vlan dengan menggunakan STP. Hasil simulasi telah ditunjukkan dan dianalisis secara menyeluruh dengan mengambil parameter yang berbeda seperti ujung ke ujung *delay*, konsumsi waktu, dan kecepatan transmisi paket. Semua parameter dihitung untuk kegagalan tautan atau perangkat dan tidak ada kegagalan. Kesimpulan dari penelitian adalah kegagalan apapun pada perangkat tidak mempengaruhi jaringan. Komunikasi antar pengguna VLAN yang sama tetap tidak terganggu. Pada FHRP, waktu rata-rata HSRP adalah 57.3 detik tanpa *link off* sedangkan dengan *link off* sebesar 86.6 detik lebih besar dari VRRP dan GLBP. *End to end delay* dari HSRP memiliki rata-rata lebih rendah daripada GLBP dan VRRP.

Penelitian Julia, dkk [7] tahun 2020 menganalisis *first hop redundancy protocol* (FHRP) berupa VRRP, HSRP, GLBP dengan menggunakan protokol *routing* BGP dan EIGRP, dimana penelitian dilakukan dengan menganalisis hasil parameter QoS berupa *throughtput*, *jitter*, *packet loss* dan *downtime*. Hasil rata-rata *throughtput* pada pengujian ini dihasilkan bahwa VRRP memiliki nilai rata-rata *throughtput* yang lebih baik daripada HSRP dan GLBP, hasil rata-rata *jitter* diketahui bahwa GLBP memiliki nilai terendah daripada HSRP dan VRRP yang berarti bahwa GLBP lebih bagus dari segi *jitter*, dan hasil rata-rata *packet loss* dapat disimpulkan bahwa GLBP memiliki nilai rata-rata *packet loss* yang paling rendah, berarti bahwa GLBP lebih baik dari segi *packet loss* daripada HSRP dan VRRP. Kemudian untuk nilai *downtime* sendiri, GLBP memiliki nilai *downtime* terendah, berarti bahwa GLBP lebih bagus dari segi *downtime* daripada HSRP dan VRRP. Berdasarkan hasil evaluasi kinerja dapat disimpulkan bahwa GLBP protokol memiliki nilai QoS terbaik dibandingkan dengan VRRP protokol dan protokol HSRP. Meskipun di uji *throughput*, GLBP memiliki nilai *throughput* terkecil.

Pada tahun 2019 Zemtsov [8] melakukan penelitian tentang analisis dari kinerja FHRP untuk jaringan komputer pada *industry enterprise*. Dari hasil penelitian didapatkan bahwa VRRP adalah protokol redudansi yang paling cepat

dalam penggunaan waktu dan memiliki konfigurasi yang lebih fleksibel Eksperimen ini dapat lebih ditingkatkan dengan mengurangi interval ping pada host linux alpine untuk meningkatkan akurasi. *open standar* juga membuat VRRP menjadi pilihan yang lebih menarik karena memungkinkan penggunaan perangkat jaringan dari vendor yang berbeda.

Pada tahun 2018 Handoko dan Isa [9] meneliti *high availability* analisis dengan *database cluster*, *load balancer*, dan *router redundancy* protokol. Penelitian ini menjelaskan mengenai performansi *high availability* pada *database cluster* di kombinasikan dengan *load balancer* dan *router redundancy* protokol. Hasil dari penelitian ini MariaDB Galera *Cluster Testing* sebagai salah satu topologi multi-*master* aktif-ke-aktif solusi *clustering* dapat berjalan dengan baik jika jumlah *node* atau *database cluster* lebih dari dua, Aplikasi *router redudancy* protokol (BCRB Galera *Cluster*) dengan penyeimbang beban (HAProxy) dalam komputasi awan (google mesin komputasi) memiliki nilai TPS (VRRP) dan beban tertinggi penyeimbang (HAProxy) bila digabungkan dengan MariaDB *Galera Cluster* memiliki ketersediaan dan kinerja yang lebih baik. dan yang terbaik waktu respons pada 32.

Tabel 2.1 Rangkuman keterkaitan dengan penulisan sebelumnya

Peneliti	Judul Penelitian	Penelitian Utama
Mudhoep,dkk	Kombinasi protokol *routing* OSPF dan BGP dengan VRRP, HSRP, dan GLBP	Penelitian ini menggunakan protokol redudansi VRRP, HSRP, dan GLBP, serta protokol *routing* OSPF dan BGP dengan parameter pengujian berupa *throughput*, *delay* dan *packet loss* pada *router* cisco
Michael,dkk	Protokol *virtual router redundancy* sebagai *backup route gateway* menggunakan *router* mikrotik	Penelitian ini menggunakan protokol redudansi VRRP, serta protokol *routing* OSPF dengan parameter pengujian berupa *throughput* dan *packet loss* pada *router* mikrotik
Dharma dkk	Kinerja protokol *network*	Penelitian ini menggunakan

Peneliti	Judul Penelitian	Penelitian Utama
	redundansi VRRP, HSRP dan GLBP pada layanan video *streaming*	protokol redudansi VRRP, HSRP, dan GLBP, dengan parameter pengujian berupa *throughput*, *delay*, *packet loss* dan waktu perpindahan *link* pada *router* cisco
Shahriar dan Fan	*Performance analysis of* FHRP *in a* VLAN *network with* STP	Penelitian ini menggunakan protokol redudansi VRRP, HSRP, dan GLBP, serta protokol STP dengan parameter pengujian berupa *time consumption*, *packet transfer rate dan end to end delay* pada *router* cisco
Julia, dkk	*Performance evaluation of First Hop Redundancy Protocol* (FHRP) *on* VRRP, HSRP, GLBP *with routing protocol* BGP *and* EIGRP	Penelitian ini menggunakan protokol redudansi VRRP, HSRP, dan GLBP, serta protokol *routing* BGP dan EIGRP dengan parameter pengujian berupa *throughput*, *jitter*, *packet loss*, dan *downtime* pada *router* cisco
Zemtsov	*Performance evaluation of first hop redundancy protocols for a computer networks of an industrial enterprise*	Penelitian ini menggunakan protokol redudansi VRRP, HSRP, dan GLBP, serta protokol *routing* RIP dengan parameter pengujian berupa *failovertime* pada *router* cisco
Handoko dan Isa	*High availability analysis with database cluster, load balancer and virtual router redudancy protocol*	Penelitian ini menggunakan protokol redudansi VRRP, *database cluster*, dan *load balancer* untuk *high availability* dengan parameter pengujian berupa *transaction*

Peneliti	Judul Penelitian	Penelitian Utama
		per second dan *response time*

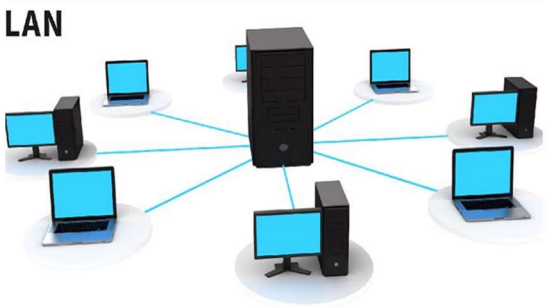
2.2 DASAR TEORI
2.3 JARINGAN KOMPUTER

Jaringan komputer merupakan sekelompok peralatan komputer yang saling terhubung untuk memungkinkan komunikasi dan berbagi sumber daya. Untuk memastikan sistem jaringan berjalan dengan teratur, aturan-aturan (protokol) yang mengatur komunikasi dan layanan-layanan secara umum diperlukan dalam suatu jaringan komputer[10]

2.4 ARSITEKTUR JARINGAN KOMPUTER

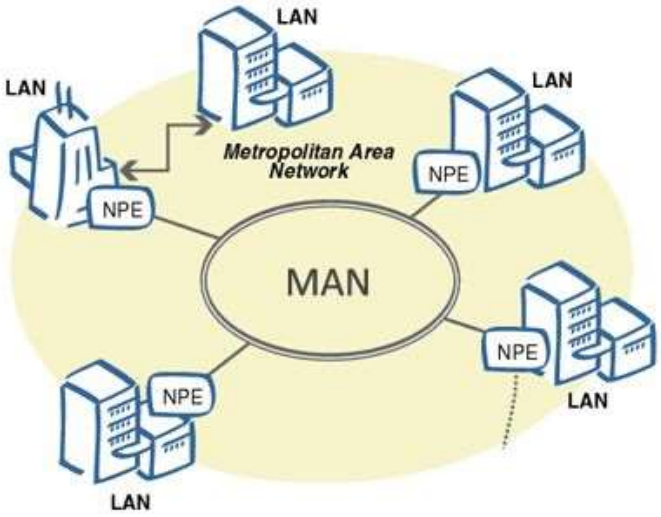
Pasa jaringan komputer terdapat arsitutektur jaringan. Arsitektur jaringan dapat dikelompokkan berdasarkan jarak dan lokasi, yang terdiri dari beberapa jenis seperti *Local Area Network* (LAN), *Metropolitan Area Network* (MAN), *Wide Area Network* (WAN).

a. *Local Area Network* (LAN) merupakan suatu arsitektur jaringan yang terdiri dari beberapa komputer yang saling terhubung dalam satu jaringan yang sama seperti ditunjukkan pada Gambar 2.1. Pada jaringan ini setiap komputer dapat saling mengakses data dari komputer lain.



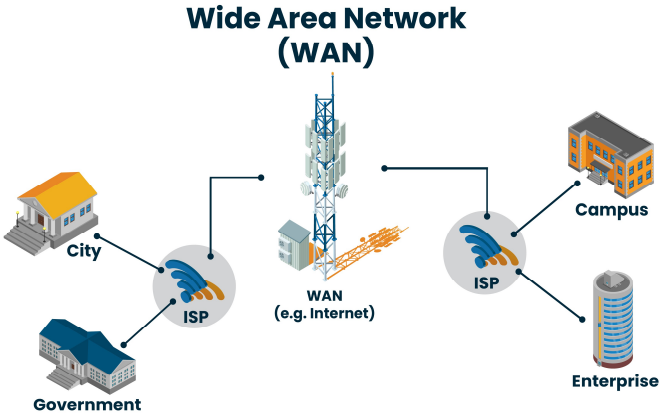
Gambar 2.1 *Local Area Network* (LAN)

b. *Metropolitan Area Network* (MAN) adalah gabungan dari beberapa jaringan LAN yang terpisah secara geografis namun dapat saling berkomunikasi menggunakan protokol *routing* seperti ditunjukkan pada Gambar 2.2.



Gambar 2.2 *Metropolitan Area Network* (MAN)

c. *Wide Area Network* (WAN) merujuk pada arsitektur jaringan yang mampu mencakup suatu area geografis yang sangat luas dengan menggunakan penyedia layanan sebagai titik utama, dimana infrastruktur nirkabel atau tanpa kabel dimanfaatkan dalam menghubungkan *site* yang berlokasi jauh satu sama lain seperti ditunjukkan pada Gambar 2.3[11]

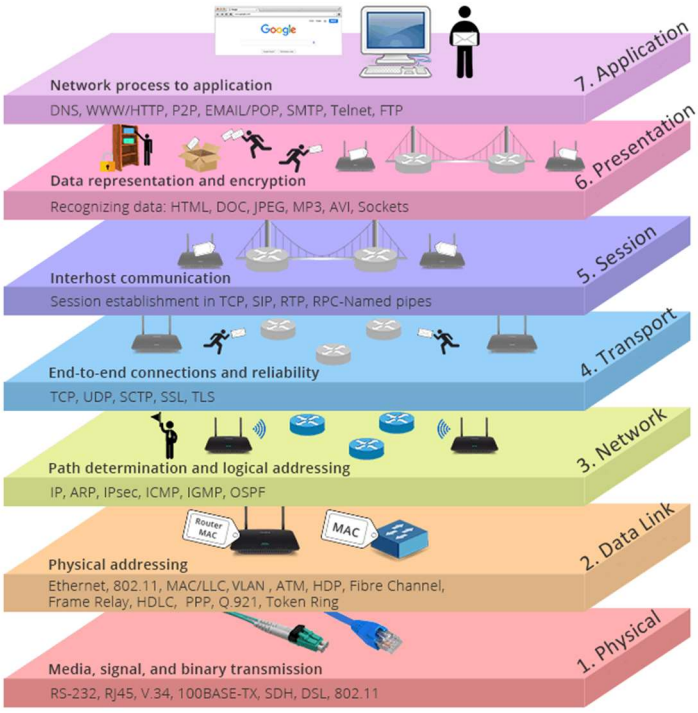


Gambar 2.3 *Wide Area Network* (WAN)

2.5 OSI LAYER

Model OSI (*Open System Interconnection*) diciptakan oleh *International Organization for Standardization* (ISO) sebagai suatu kerangka logika terstruktur yang bertujuan untuk menjelaskan proses komunikasi data melalui jaringan. Sebelumnya, proses komunikasi data melibatkan komputer-komputer yang berasal dari vendor yang berbeda dan masing-masing vendor menggunakan protokol serta format data yang berbeda-beda. Kondisi tersebut mendorong ISO untuk

mengembangkan sebuah arsitektur komunikasi yang disebut dengan model OSI sebagaimana ditunjukkan Gambar 2.4, yang bertujuan untuk menetapkan standar dalam menghubungkan komputer-komputer dari vendor yang berbeda [12].



Gambar 2.4 Osi Layer Model

Secara umum, fungsi dan penjelasan masing-masing *layer* adalah sebagai berikut :

a. Physical Layer

Physical layer berperan dalam mendefinisikan berbagai aspek dalam jaringan, termasuk media transmisi, sinkronisasi bit, arsitektur jaringan (seperti Ethernet), topologi jaringan, dan pengabelan. Selain itu, *layer* ini menetapkan cara interaksi *Network Interface Card* (NIC) dengan media kabel atau radio. Data biner diubah menjadi bentuk yang dapat ditransmisikan melalui media jaringan seperti kabel, *transceiver*, dan konektor yang terkait dengan *Physical layer*. Komponen jaringan seperti *repeater*, hub, dan kartu jaringan juga terletak pada *layer* ini [12].

b. Data-*link* layer

Dalam jaringan komputer, terdapat suatu *layer* yang bertanggung jawab dalam menentukan bagaimana bit-data dikelompokkan menjadi suatu format yang

disebut sebagai *frame*. Selain itu, pada level ini terdapat fungsi-fungsi seperti koreksi kesalahan, *flow control*, dan pengalamatan perangkat keras (seperti *Media Access Control Address* atau MAC *Address*)[12].

c. Network Layer

Lapisan Jaringan berfungsi untuk mengatur alamat IP dan fungsi *routing* sehingga paket data dapat dikirim dari jaringan lokal ke jaringan tujuan lainnya. Protokol IP digunakan sebagai contoh dalam lapisan ini [12].

d. Transport Layer

Dalam *layer* transport, data dipecah menjadi paket-paket data dan diberikan nomor urut pada setiap paket sehingga dapat dirangkai kembali pada sisi penerima setelah diterima. Selain itu, pada level ini juga dibuat tanda penerimaan paket yang berhasil (*acknowledgement*) dan melakukan retransmisi terhadap paket-paket yang hilang di tengah jalan.

Protokol yang digunakan pada level *transport* data antara lain UDP dan TCP. *Layer* ini bertanggung jawab untuk menyediakan transfer yang handal dan transparan antara kedua titik akhir, serta melakukan *multiplexing*, kendali aliran, pemeriksaan kesalahan dan perbaikan.[12].

e. Session Layer

Layer session digunakan untuk menentukan bagaimana koneksi antara dua perangkat dapat dimulai, dipertahankan, atau diakhiri. Pada *layer session* terdapat beberapa protokol yang digunakan antara lain NETBIOS, NETBEUI, ADSP, dan PAP. *Layer session* juga bertanggung jawab untuk mengontrol dialog antara aplikasi pada komputer yang berbeda serta menyediakan pengelolaan token dan sinkronisasi data[12].

f. Presentation Layer

Presentation Layer memiliki fungsi untuk mengubah format data dari aplikasi menjadi format yang dapat ditransmisikan melalui jaringan. Pada level ini terdapat protokol yang disebut dengan perangkat lunak redirektor (*redirector software*), seperti layanan *Workstation* yang terdapat pada Windows NT dan

Network shell seperti *Virtual Network Computing* (VNC) atau *Remote Desktop Protocol* (RDP). Redirektor *software* ini bertanggung jawab untuk mengumpulkan data dari aplikasi dan mentransformasikannya ke dalam format yang dapat dikirim melalui jaringan, serta mengembalikan data yang diterima ke dalam format yang dapat diproses oleh aplikasi penerima. Selain itu, *Presentation Layer* juga mengatur enkripsi dan dekripsi data untuk menjaga keamanan data saat ditransmisikan melalui jaringan[12].

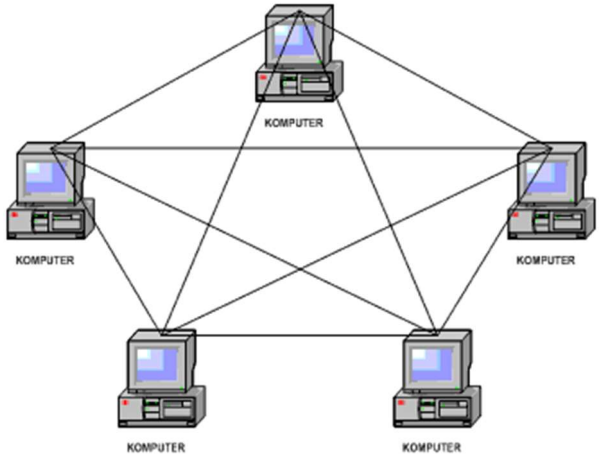
g. Aplication Layer

Layer Aplikasi berfungsi sebagai antarmuka antara aplikasi dengan jaringan, yang mengatur bagaimana aplikasi dapat mengakses jaringan dan memberikan pesan kesalahan. Protokol yang berada di lapisan ini, seperti HTTP, FTP, SMTP, dan NFS, memungkinkan aplikasi untuk berkomunikasi dengan jaringan dan memanfaatkan fungsionalitas jaringan untuk keperluan aplikasi tersebut. Dengan demikian, *Layer* Aplikasi menjadi lapisan yang paling dekat dengan pengguna akhir, karena langsung terkait dengan aplikasi yang digunakan oleh pengguna[12].

2.6 TOPOLOGI JARINGAN

a. Topologi Jaringan Mesh

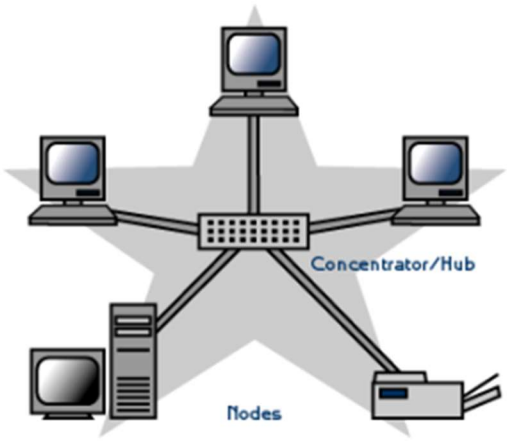
Topologi jaringan *mesh* adalah jenis topologi jaringan dimana setiap sentral terhubung dengan sentral lain secara langsung dan terdapat hubungan antara setiap pasang sentral yang ada. Semakin banyak sentral yang terhubung, semakin kompleks jaringannya yang dapat dilihat pada Gambar 2.5. Meskipun demikian, topologi ini memiliki keunggulan karena memiliki tingkat redundansi yang tinggi, sehingga keandalan jaringannya cukup baik. Namun, pengoperasian topologi ini memerlukan biaya yang relatif mahal dibandingkan dengan topologi jaringan lainnya [13].



Gambar 2.5 Topologi Jaringan *Mesh*

b. Topologi Jaringan Star

Topologi jaringan *star* menggunakan satu perangkat sebagai pusat atau sentral, di mana semua perangkat lain terhubung ke sentral tersebut sebagaimana ditunjukkan seperti pada Gambar 2.6. Dalam hal kerumitan jaringan, topologi *star* lebih sederhana dibandingkan dengan topologi *mesh*, sehingga lebih ekonomis. Namun, sentral pusat dalam topologi *star* memikul beban yang cukup besar, yang dapat meningkatkan risiko kerusakan dan gangguan dalam jaringan[13].

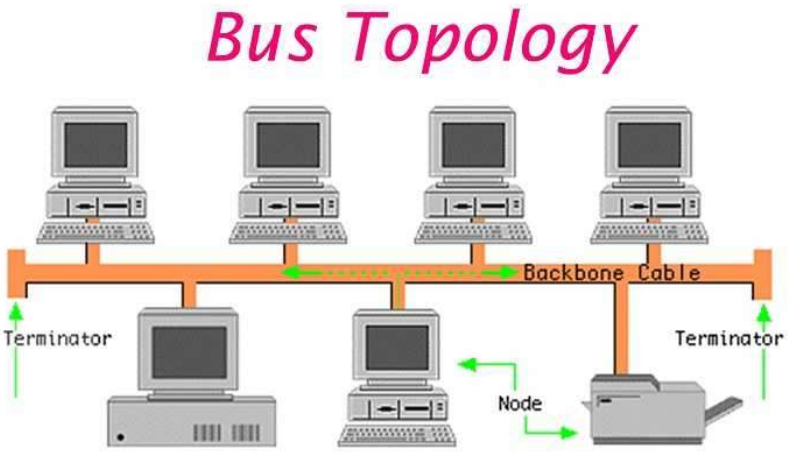


Gambar 2.6 Topologi Jaringan *Star*

c. Topologi Jaringan Bus

Topologi jaringan *bus* menghubungkan semua perangkat langsung ke media transmisi dalam sebuah konfigurasi yang disebut *bus* sebagaimana

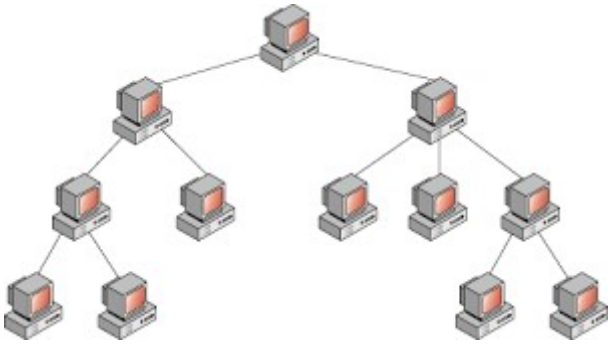
ditunjukkan pada Gambar 2.7. Transmisi sinyal hanya dapat dilakukan dalam satu arah pada satu waktu, tidak seperti pada topologi jaringan *mesh* atau *star* yang dapat melakukan komunikasi antara perangkat secara simultan. Topologi jaringan *bus* tidak sering digunakan untuk menghubungkan perangkat, namun biasanya digunakan dalam jaringan komputer[13].



Gambar 2.7 Topologi Jaringan *Bus*

d. Topologi Jaringan Tree

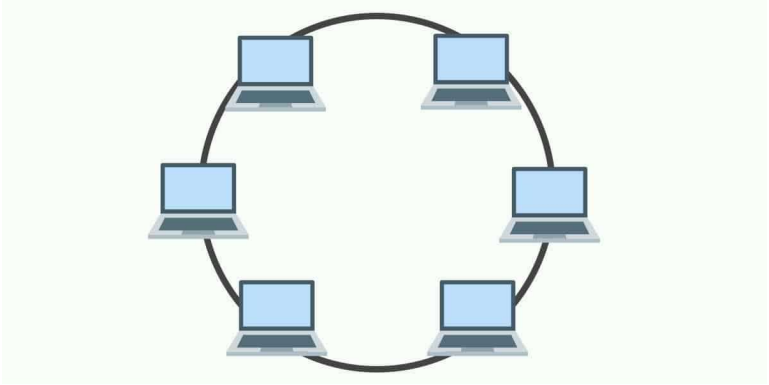
Topologi jaringan *tree*, atau juga dikenal sebagai topologi bertingkat, digunakan untuk menghubungkan perangkat dengan hierarki yang berbeda ditunjukkan pada Gambar 2.8. Hierarki yang lebih rendah direpresentasikan oleh lokasi yang lebih rendah dalam struktur, dan semakin tinggi hierarkinya, semakin tinggi juga posisinya dalam struktur. Topologi ini umumnya digunakan untuk sistem jaringan komputer [13].



Gambar 2.8 Topologi Jaringan *Tree*

e. Topologi Jaringan Ring

Untuk membentuk jaringan dengan topologi jaringan *ring*, setiap perangkat harus dihubungkan secara seri satu sama lain membentuk *loop* tertutup sebagaimana terlampir pada Gambar 2.9. Dalam sistem ini, setiap perangkat memiliki kemampuan untuk berinteraksi dengan perangkat yang berdekatan dan berjauhan, sehingga dapat melakukan *switch*ing ke berbagai arah. Keuntungan dari topologi ini adalah jaringannya sederhana, dan jika ada gangguan atau kerusakan pada satu perangkat, aliran data masih dapat dilanjutkan pada arah lain dalam sistem[13].



Gambar 2.9 Topologi Jaringan *Ring*

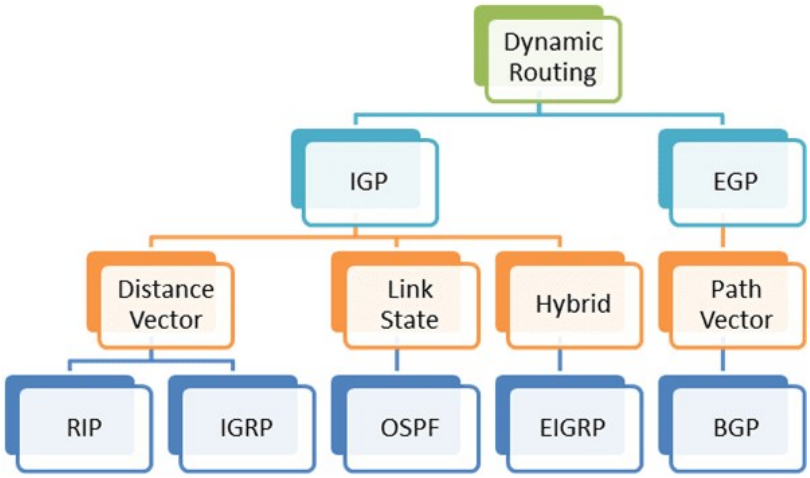
2.7 VIRTUAL ROUTER REDUDANCY PROTOCOL

Virtual Router Redundancy Protocol (VRRP) adalah protokol standar terbuka yang dapat digunakan pada perangkat dari berbagai vendor. Konsep VRRP hampir sama dengan HSRP, namun memiliki beberapa perbedaan. VRRP memungkinkan konfigurasi kelompok pada beberapa *router*, di mana salah satu di antaranya akan menjadi *router master* dan lainnya akan bertindak sebagai *backup*.

Ketika *router master* mengalami *down* atau *link* failure, *router backup* akan mengambil alih peran sebagai *router master*. Protokol ini digunakan untuk mempertahankan komunikasi dengan menerapkan sistem redundansi pada *router*, sehingga *down* komunikasi dapat dihindari dan proses komunikasi kepada pelanggan tetap terjaga. Pada umumnya, VRRP menggunakan *router* cluster dengan salah satu *router* aktif sebagai pengatur proses *routing*, dan *router* lainnya siap untuk mengambil alih peran aktif jika terjadi masalah pada *router* utama[14].

2.8 ROUTING DINAMIS

Routing dinamis adalah teknik *routing* di mana *router* secara otomatis memasukkan entri rute ke dalam tabel *routing* dengan menukar informasi tentang jaringan yang mereka ketahui. *Router* akan membuat entri rute setelah mempelajari keberadaan dan cara mencapai jaringan lain, dan kemudian memasukkannya ke dalam tabel *routing*. Untuk melakukan pertukaran informasi *routing*, *router* harus menggunakan protokol *routing* yang sama jika ingin bertukar informasi dengan *router* lain. Routing Dinamis dibagi menjadi dua secara umum yaitu IGP dan EGP terlihat seperti pada Gambar 2.10 [15].



Gambar 2.10 *Dynamic Routing*

2.9 BORDER GATEWAY PROTOCOL

BGP adalah protokol perutean yang digunakan dalam perutean antar domain sistem dalam dua mode, iBGP dan eBGP. Itu dianggap sebagai *de facto* dasar protokol *routing* untuk internet dan dengan demikian hadir di sebagian besar

router eksternal atau edge. BGP adalah vektor jalur algoritma yang digunakan untuk berbagi informasi *routing* dan *reachability* antara AS. BGP adalah *Open Systems Interconnection* (OSI) protokol lapisan transport yang mendukung antar-domain tanpa kelas perutean (CIDR). Intinya, BGP adalah protokol *routing* yang memungkinkan internet dengan mengidentifikasi jalur antara AS dan oleh meneruskan informasi perutean dan keterjangkauan ke AS yang berdekatan.

BGP memanfaatkan informasi ASN yang terkait dengan AS untuk menentukan rute yang akan digunakan. Selain itu, BGP memperoleh informasi *routing* dan *reachability* dari BGP yang berdekatan *gateway*. Informasi perutean disimpan di perangkat tabel *routing* dan dengan demikian digunakan untuk meneruskan paket antara AS. Internet adalah jaringan yang besar dan kompleks, dengan topologi perubahan yang terjadi terus-menerus. Pembaruan BGP, oleh karena itu, terjadi dengan kecepatan yang meningkat. Akibatnya, internet tidak lagi mencapai kondisi stabil; selalu ada pembaruan BGP yang terjadi di suatu tempat. Penting untuk dicatat bahwa BGP tidak menyiarkan alamatnya dan sebagai gantinya mengandalkan pembaruan rutin dari router yang berdekatan[16].

2.10 AUTONOMOUS SYSTEM NUMBER

Autonomous System Number (ASN) adalah pengidentifikasi unik global yang menentukan grup dari satu atau lebih prefiks IP yang dijalankan oleh satu atau lebih operator jaringan yang mempertahankan satu kebijakan perutean yang ditentukan dengan jelas. Kelompok awalan IP ini dikenal sebagai sistem otonom. ASN memungkinkan sistem otonom untuk bertukar informasi perutean dengan sistem otonom lainnya. Terdapat dua jenis ASN, yaitu ASN privat dan ASN publik. ASN pribadi dapat digunakan untuk sistem yang berkomunikasi melalui BGP (*Border Gateway Protocol*) dengan satu penyedia, sedangkan ASN publik diperlukan untuk bertukar informasi melalui Internet[17].

2.11 VYOS

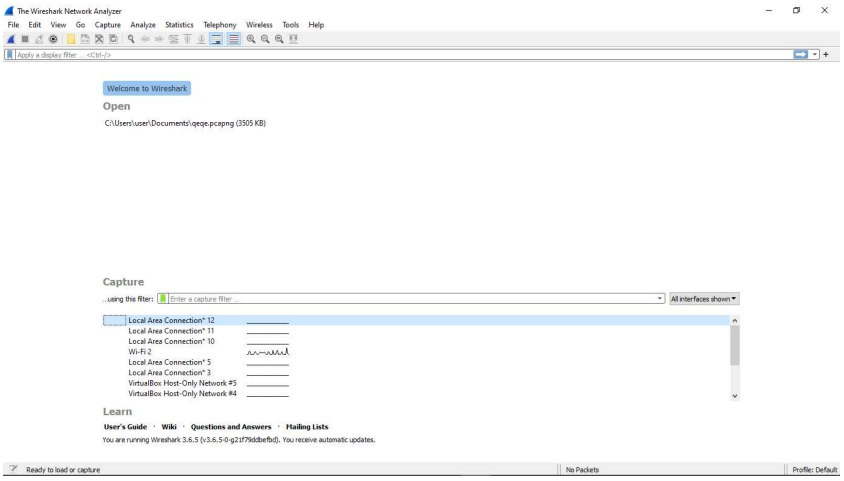
VyOS adalah salah satu sistem operasi *open* source yang berbasi kernel Linux Debian yang memiliki fitur utama sebagai *routing*, *firewall*, dan VPN. Sistem ini menawarkan antarmuka CLI yang dapat disesuaikan dengan model *router hardware* tertentu dan dapat dikonfigurasi menggunakan skrip. Konfigurasi

sistemnya bersifat *stateful* yang memungkinkan pengguna untuk membaca, menulis, menghapus, dan mengeksekusi konfigurasi secara fleksibel. Selain itu, VyOS juga memiliki kemampuan untuk melakukan pembaruan sistem operasi dan menyediakan bahasa kebijakan *routing* yang kompleks, termasuk protokol *routing* seperti BGP dan OSPF. Sistem VyOS juga dapat dijalankan pada *platform virtual* maupun fisik. Konfigurasi dilakukan melalui CLI, dan setiap perintah yang dimasukkan akan dieksekusi oleh sistem. Gambar dari sesi CLI ditunjukkan pada Gambar 2.11 [18].

Gambar 2.11 VyOS Router OS

2.11 WIRESHARK

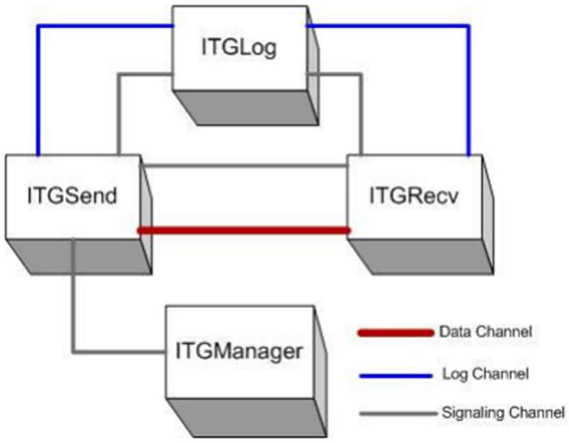
Wireshark merupakan perangkat analisis paket yang dapat digunakan secara bebas dan memiliki sumber terbuka. Alat ini berguna untuk memecahkan masalah dalam jaringan, melakukan analisis, mengembangkan perangkat lunak dan protokol komunikasi, serta digunakan untuk tujuan pendidikan. Sebagai salah satu aplikasi *Network Analyzer* yang populer, Wireshark banyak digunakan oleh *Network Administrator* untuk mengawasi kinerja jaringan dan mengatur lalu lintas data yang mengalir di jaringan yang mereka kelola. Dalam mengoperasikan tugasnya, Wireshark mampu menangkap berbagai jenis paket data yang mengalir di jaringan, termasuk yang berformat protokol yang berbeda ditunjukkan pada Gambar 2.12 [19].



Gambar 2.12 *Software Wireshark*

2.12 D-ITG

Distributed Internet Traffic Generator (D-ITG) merupakan sebuah *platform* atau *software* yang dapat menghasilkan lalu lintas IPv4 dan IPv6 dengan akurasi tinggi untuk mereplikasi beban kerja aplikasi internet saat ini. Selain itu, D-ITG juga berfungsi sebagai alat yang dapat mengukur kinerja umum seperti *throughput*, *delay*, *jitter*, dan *packet loss* pada tingkat paket. D-ITG dapat menghasilkan lalu lintas yang mengikuti model stokastik untuk ukuran paket dan waktu antar keberangkatan yang meniru perilaku protokol tingkat aplikasi.



Gambar 2.13 Arsitektur D-ITG

1. **ITG *Send***

   ITG *Send* seperti pada Gambar 2.13 dapat menghasilkan *file* log yang menjelaskan setiap aliran yang dikirim pada tingkat paket. *File* log tersebut dapat disimpan secara lokal atau jarak jauh menggunakan *server* log ITGLog.

2. **ITG *Recv***

ITG *Recv* seperti pada Gambar 2.13 menghasilkan *file* log yang menjelaskan setiap aliran yang diterima pada tingkat paket. *File* log tersebut dapat disimpan secara lokal atau jarak jauh menggunakan *server* log ITGLog, seperti yang dijelaskan di website resminya[20].

2.13 EVE-NG

EVE-NG ditunjukkan pada Gambar 2.14 adalah sebuah alat yang digunakan untuk menghubungkan perangkat virtual dan fisik, serta menyediakan banyak fitur yang menyederhanakan penggunaan, pengelolaan, distribusi, dan kemampuan untuk memahami dan berbagi topologi, pekerjaan, ide, dan konsep. Alat ini dapat mengurangi biaya dan waktu yang dibutuhkan untuk mengatur sebuah laboratorium, bahkan memungkinkan tugas-tugas yang sebelumnya tidak terpikirkan. EVE-NG dapat digunakan untuk mempelajari semua jenis teknologi, baik umum maupun khusus vendor, termasuk teknologi baru seperti otomatisasi jaringan dan SDN. Selain itu, EVE-NG juga dapat digunakan untuk mereplikasi jaringan perusahaan dan menguji perubahan sebelum diterapkan secara langsung pada produksi[21].

Gambar 2.14 EVE-NG

2.14 QUALITY OF SERVICE

Quality of Service (QoS) adalah sebuah pendekatan untuk menilai seberapa baik sebuah jaringan komputer, yang melibatkan penentuan karakteristik dan atribut dari suatu layanan. QoS digunakan untuk mengevaluasi serangkaian kinerja yang telah ditentukan dan dikaitkan dengan layanan tertentu, dengan tujuan untuk memfasilitasi lalu lintas jaringan komputer secara lebih efektif

dengan teknologi yang berbeda. berikut persentase penilaian dari QoS ditujukkan pada Tabel 2.2.

Tabel 2.2 Indeks parameter QoS

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

Dalam menentukkan QoS terdapat parameter-parameter yang digunakan antara lain *Throughput*, *Delay*, *Jitter* dan *Packet Loss*. Parameter-parameter penilaian ini berdasarkan *Telecommunications* and Internet *Protokol Harmonization Over Network*s (TIPHON). TIPHON merupakan standar yang digunakan sebagai penilaian QoS yang dikeluarkan oleh badan standar *European Telecommunications Standard*s *Institute* (ETSI). Berikut penjelasan parameter-parameter QoS sebagai berikut [22].

1. **Throughput**

Throughput adalah ukuran *bandwidth* aktual yang diperoleh selama suatu periode waktu tertentu ketika mentransmisikan *file* sebagaimana terlihat pada persamaan 2.1. Selain itu, *throughput* juga mencerminkan total jumlah paket yang diterima secara sukses selama periode waktu tertentu dan kemudian dibagi dengan durasi interval waktu tersebut. Berdasarkan standar TIPHON kategori dalam throughput dapat dilihat pada Tabel 2.3[22].

Tabel 2.3 Kategori *throughput*

Kategori *Throughput*	*Throughput*	Indeks
Sangat Bagus	> 2.1 Mbps	4
Bagus	1200 Kbps – 2.1 Mbps	3
Cukup	700 – 1200 Kbps	2
Kurang Bagus	338 – 700 Kbps	1
Tidak Bagus	0 – 338 Kbps	0

Perhitungan *Throughput* :

$$Throughput = \frac{Jumlah\ data\ yang\ dikirim\ (kb)}{Waktu\ Pengiriman\ data\ (s)} \qquad (2.1)$$

2. **Delay**

Delay merupakan ukuran kualitas layanan jaringan yang menunjukkan jumlah waktu yang dibutuhkan oleh paket dalam melakukan perjalanan dari sumber menuju tujuan sebagaimana persamaan 2.2. Beberapa faktor dapat dipengaruhi *delay* seperti perangkat keras yang digunakan, jarak yang harus ditempuh, serta tingkat kepadatan lalu lintas pada jaringan. Standar *delay* berdasarkan versi TIPHON ditunjukan pada Tabel 2.4 [22].

Tabel 2.4 Kategori *delay*

Kategori *Delay*	*Delay*	Indeks
Sangat Bagus	< 150 ms	4
Bagus	150 s/d 300 ms	3
Sedang	300 s/d 450 ms	2
Tidak Bagus	> 450 ms	1

Perhitungan *Delay* :

$$Delay = \frac{Jumlah\ delay}{Jumlah\ paket\ diterima} \qquad (2.2)$$

3. **Jitter**

Ketika data ditransmisikan melalui jaringan, ada banyak variasi *delay* yang dapat terjadi, terutama dalam bentuk *jitter*. *Jitter* disebabkan oleh *delay* antrian yang terjadi pada *router* maupun *switch*, karena adanya variasi waktu dalam pengolahan paket, panjang antrian, dan waktu pengumpulan ulang paket yang sebagaimana persamaan 2.3. Kategori standar TIPHON kinerja jaringan nilai *jitter* pada Tabel 2.5 [22].

Tabel 2.5 Kategori *jitter*

Kategori *Jitter*	*Jitter*	Indeks
Sangat Bagus	0 ms	4
Bagus	0 s/d 75 ms	3

Kategori *Jitter*	*Jitter*	Indeks
Sedang	75 s/d 125 ms	2
Tidak Bagus	125 s/d 225 ms	1

Perhitungan *Jitter* :

$$Jitter = \frac{Jumlah\ variasi\ delay}{Jumlah\ paket\ diterima} \qquad (2.3)$$

4. **Packet Loss**

Parameter *packet loss* digunakan untuk menjelaskan situasi di mana sejumlah paket data hilang, biasanya disebabkan oleh kejadian *collision* dan *congestion* pada jaringan sebagaimana persamaan 2.4. Kondisi tersebut dapat berdampak pada seluruh aplikasi yang terhubung, karena retransmisi data yang hilang akan menurunkan efisiensi jaringan secara keseluruhan, bahkan jika aplikasi memiliki *bandwidth* yang cukup. Berikut merupakan kategori *packet loss* menurut versi TIPHON seperti pada Tabel 2.6 [22].

Tabel 2.6 Kategori *packet loss*

Kategori *Packet Loss*	*Packet Loss*	Indeks
Sangat Bagus	0 %	4
Bagus	3 %	3
Sedang	15 %	2
Tidak Bagus	25 %	1

Perhitungan *Packet Loss* :

$$Packet\ Loss = \frac{(Paket\ data\ dikirim - Paket\ data\ diterima)}{Paket\ data\ dikirim}\ x\ 100\ \% \qquad (2.4)$$