BAB 2
DASAR TEORI

2.1 KAJIAN PUSTAKA

Tujuan penelitian yang dilakukan oleh Nanda Gusti Arirapha berjudul "Analisis Penerapan *Access Control List* (*ACL*) sebagai Pembatasan Hak Akses pada Jaringan Berbasis *VLAN Trunking Protocol* (*VTP*)" adalah merancang jaringan *Virtual Local Area Network* (*VLAN*) berbasis *VLAN Trunking Protocol* (*VTP*) dengan menggunakan keamanan *Access Control List* (*ACL*). Selain itu, penelitian ini juga bertujuan untuk mengamati performansi jaringan yang telah dibuat dengan dan tanpa penggunaan *ACL*. Pada penelitian ini, *ACL* yang digunakan terdiri dari dua jenis yaitu *standard ACL* yang diterapkan pada *VLAN* 20, dan *extended ACL* yang diterapkan pada *VLAN* 30.[9].

Penelitian [2] dengan judul "Implementasi *Access Control List* dalam Perancangan *Virtual Local Area Network* pada PT Cakramedia *Indocyber*", membahas tentang cara mengatasi keterbatasan sumber daya jaringan dengan menggunakan pendekatan yang bijaksana dalam penggunaan sumber daya, termasuk pembatasan dan prioritas penggunaan untuk kepentingan utama perusahaan. Dalam upaya mencapai tujuan tersebut, penelitian ini menerapkan *Virtual Local Area Network* (*VLAN*) dan *switch port security* untuk membatasi akses pengguna antar jaringan di perusahaan. Selain itu, pengaturan akses *router access list* (*ACL*) juga diimplementasikan untuk mengizinkan hanya data yang relevan sesuai dengan kebutuhan komunikasi perusahaan. Dalam penelitian ini, digunakan *ACL extended* untuk memblokir koneksi *VLAN* 20 agar tidak dapat terhubung atau melakukan *ping* ke *VLAN* 40. Penelitian ini mengadopsi metode observasi dan wawancara untuk mengidentifikasi masalah yang ada di perusahaan serta menganalisis ketersediaan dan kebutuhan perangkat keras jaringan. Selain itu, penelitian juga dilakukan untuk menemukan solusi konfigurasi yang sesuai.

Penelitian [6], yang dilakukan pada tahun 2019 berjudul "Implementasi *Spanning Tree Protocol* (*STP*), *Virtual LAN* (*VLAN*), dan *Access List* (*ACL*) pada Jaringan Komputer Balai Besar Pelatihan Kesehatan Jakarta". Penelitian ini

mengeksplorasi penggunaan jaringan komputer sebagai sarana penunjang pekerjaan di Balai Besar Pelatihan Kesehatan Jakarta, yang menggunakan jaringan *Local Area Network* (*LAN*). Beberapa permasalahan yang dihadapi adalah seringnya terjadi *looping* pada perangkat *switch* yang mengakibatkan lambatnya koneksi internet. *Looping* ini berhasil diatasi dengan menerapkan metode *Spanning Tree Protocol* (*STP*) untuk menghentikannya. Selain itu, permasalahan lain adalah kurangnya batasan akses antar divisi yang memungkinkan pengguna tidak diizinkan mengakses *data* pada BBPK, sehingga berpotensi menyebabkan kebocoran data. Untuk mengatasi masalah ini, penulis menerapkan fitur *Access List* (*ACL*) pada perangkat *Router* untuk membatasi akses ke server berdasarkan batasan yang ditetapkan. Pada penelitian ini, *ACL extended* digunakan untuk membatasi akses *VLAN* 10 dan 20 ke server.

Penelitian [1] dengan judul "Perancangan Jaringan *Virtual LAN* Menggunakan Metode Protokol *VLAN Spanning Tree* bertujuan untuk merancang jaringan *VLAN* dan menerapkan jalur redundansi agar dapat membagi *segment* jaringan pada setiap divisi dengan teknologi pencegahan *broadcast storm*. Penerapan *VLAN Trunking Protocol* berhasil membagi *segment* jaringan antar divisi dengan baik, sehingga terdapat jalur *backup* antar *switch* untuk menjaga konektivitas jaringan ketika salah satu jalur mengalami gangguan.

Pada penelitian ini bertujuan untuk Mengetahui perancangan jaringan *Virtual Local Area Network* (*VLAN*) berbasis *Spanning Tree Protocol* (*STP*) dengan keamanan menggunakan *Extended Access Control List* (*ACL*). Dengan melakukan uji *ping* dan akses web server sebelum dan sesudah di terapkannya *Extended ACL*, *protocol* yang di blok pada pengujian ini ialah *HTTP* dan *ICMP*.

Tabel 2.1 berisi perbandingan antara penelitian sebelumnya dengan penelitian yang dilakukan dalam studi ini.

Tabel 2.1 Kajian Penelitian Sebelumnya

No	Nama Peneliti	Judul Penelitian	*ACL* yang digunakan	*Simulator*	*VLAN*	Hasil
1	Nanda Gusti Arirapha. 2022	Analisis Penerapan *Acces Control*	*standard ACL* dan	*GNS3*	Ya	Pengujian *QoS* setelah *Access Control List*

No	Nama Peneliti	Judul Penelitian	*ACL* yang digunakan	*Simulator*	*VLAN*	Hasil
		List (*ACL*) Sebagai Pembatasan Hak Akses Pada Jaringan Berbasis *Vlan trunking Protocol* (*VTP*)	*Extended ACL*			diterapkan dapat diketahui perfomansi paling baik berada pada koneksi *VLAN* 10 terhadap publik dengan standar sangat baik sedangkan nilai *QoS* paling buruk berada pada konektivitas *VLAN* lokal – publik, *vlan* lokal – *vlan* 10 dengan
2	Fahrizal, Bayu Arikha Candra. 2022	Implementasi *Access Control List* Dalam Perancangan *Virtual Local Area Network* Pada Pt Cakramedia *Indocyber*	*ACL extended*	*Cisco Packet Tracer*	Ya	Test *ping* yang dilakukan penulis setelah *ACL* diterapkan berhasil memfilter data mana yang di izinkan atau di tolak
3	Hafdiarsya Saiya, Mohammad Noviansyah. 2019	Implementasi *Spanning Tree Protocol* (*Stp*), *Virtual Lan* (*Vlan*), Dan *Access List* (*Acl*)	*Standar ACL*	*Cisco Packet Tracer*	Ya	Setelah mengaktifkan fitur *Access List* pada *router* dapat membatasi *vlan* 10 dan 20 yang menggunakan

No	Nama Peneliti	Judul Penelitian	*ACL* yang digunakan	*Simulator*	*VLAN*	Hasil
		Pada Jaringan Komputer Balai Besar Pelatihan Kesehatan Jakarta				server dan mencegah user mengambil data dari divisi lain.
4	Adi Sopian, Khusnul Khoiriyah, Ilham Dwi Putra Gonti 2022	Perancangan Jaringan *Virtual Lan* Menggunakan Metode Protokol Peer-*Vlan Spanning Tree*	-	*Cisco Packet Tracer*	Ya	Supaya proses pengiriman data dapat bekerja dengan baik tanpa mengalami *broadcast storm* atau *loop* perlu di terapkannya *STP* dan VTP pada perusahaan XYZ
5	Lutfi Halwani	Analisis Penerapan *Acces Control List* (*Acl*) Sebagai Pembatasan Hak Akses Pada Jaringan *Vlan Spanning Tree Protocol* (*Stp*)	*Extended ACL*	*Eve-NG*	Ya	*Vlan* 10 setelah dibatasi hak akses dengan *protocol icmp* dan *http* tidak bisa mengakses ke server satu namun masih bisa mengakses ke server dua sedangkan *vlan*20 dapat mengakses ke dua server tersebut

2.2 DASAR TEORI

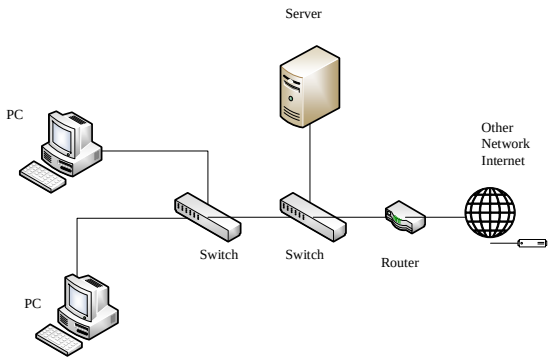
2.2.1 JARINGAN KOMPUTER

Jaringan komputer merupakan suatu struktur terdiri dari komputer-komputer, perangkat lunak, dan perangkat jaringan yang berkolaborasi untuk mencapai tujuan tertentu. Untuk mencapai tujuan tersebut, setiap elemen dalam jaringan memiliki peran khusus dalam menerima dan mengirimkan layanan-layanan yang diperlukan. Pihak yang menggunakan sumber daya dari server disebut sebagai klien (*client*), sedangkan pihak yang menyediakan berbagai jenis layanan disebut sebagai pelayan (server). Model ini dikenal dengan istilah arsitektur *client*-server dan umumnya digunakan dalam hampir semua aplikasi jaringan komputer. Jaringan komputer terdiri dari dua atau lebih komputer yang saling terhubung untuk pertukaran data. Keberadaan jaringan komputer merupakan gabungan antara perangkat keras (*hardware*) dan perangkat lunak (*software*)[10]**.**

Jaringan komputer memiliki banyak objek di dalamnya, dan setiap objek memiliki perannya masing-masing. Beberapa objek yang akan disebutkan antara lain:

1. Komputer
2. Kabel LAN
3. *Switch*/*Router*

Ketiga perangkat tersebut membentuk *unit* terkecil dari suatu jaringan komputer yang sederhana. Komunikasi antara beberapa komputer yang saling terhubung ini menciptakan sistem yang utuh yang dikenal sebagai jaringan komputer, Gambar 2.1 menunjukan jaringan komputer sederhana[11].

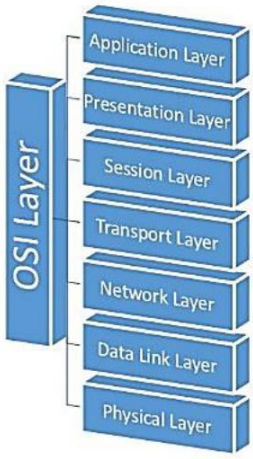


Gambar 2.1 Jaringan Komputer

Seorang pengguna komputer akan mendapatkan kemudahan jika mereka dapat bertukar file dalam suatu jaringan komputer, melakukan komunikasi melalui *chat*, berbagi printer, dan melakukan aktivitas lainnya yang terkait dengan kegiatan sosial pengguna komputer tersebut. Oleh karena itu, kebutuhan akan jaringan komputer menjadi semakin kompleks seiring dengan meningkatnya ragam layanan yang dibutuhkan oleh para pengguna komputer[11].

2.2.2 *OSI* (*Open System Interconnection*)

OSI (*Open System Interconnection*) adalah protokol standar komunikasi data yang dikeluarkan oleh *ISO* (*International Organization for Standardization*) dan diakui sebagai acuan utama oleh berbagai badan standarisasi di seluruh dunia. Sebagai standar yang sangat terpercaya, *OSI* memastikan interoperabilitas yang efisien antara perangkat dan jaringan yang berbeda. Meskipun suatu badan standarisasi mungkin mengeluarkan protokol yang tidak memiliki 7 *layer*, tetapi protokol tersebut harus tetap memenuhi fungsi-fungsi dari ketujuh *layer* dalam model *OSI*. Protokol *OSI* terdiri dari 7 *layer*, yang juga dikenal sebagai *Layer OSI*. Dengan peran yang khusus ini, tiap *layer* berkontribusi pada keberhasilan komunikasi yang andal dan efisien dalam lingkungan jaringan yang kompleks.



Gambar 2.2 *OSI Layer*[12]

Gambar 2.2 menampilkan 7 *layer OSI*, yang juga dikenal sebagai *OSI Layer*, dengan masing-masing memiliki fungsi sendiri. *Layer* tersebut terdiri dari

Physical, Data Link, Network, Transport, Sessions, Presentation, dan *Applications*. Berikut adalah fungsi dari setiap *layer*:

1. *Layer* 1: *Physical*

   Fungsi: Melakukan transmisi bit stream melalui media transmisi.

   Contoh: 100Base-T, GB, STM-1, DSL, UTP.

2. *Layer* 2: *Data Link*

   Fungsi: Merespons transmisi yang bebas dari kesalahan, menentukan koneksi secara logik antar stasiun.

   Contoh: ATM, IEEE 802.1Q, PPP, LLC, MAC.

3. *Layer* 3: *Network*

   Fungsi: Melakukan pengalamatan dan *routing*.

   Contoh: IP, RIP.

4. *Layer* 4: *Transport*

   Fungsi: Mentransportasikan data secara *end to end*, melakukan *flow control*, menyediakan transmisi yang handal.

   Contoh: *TCP*, UDP.

5. *Layer* 5: *Sessions*

   Fungsi: Mendukung koneksi antar sesi, membuat, mengelola, dan mengakhiri koneksi.

   Contoh: RADIUS.

6. *Layer* 6: *Presentation*

   Fungsi: Menangani format data.

   Contoh: ASCII, MPEG, JPEG, DNS, *HTTP*.

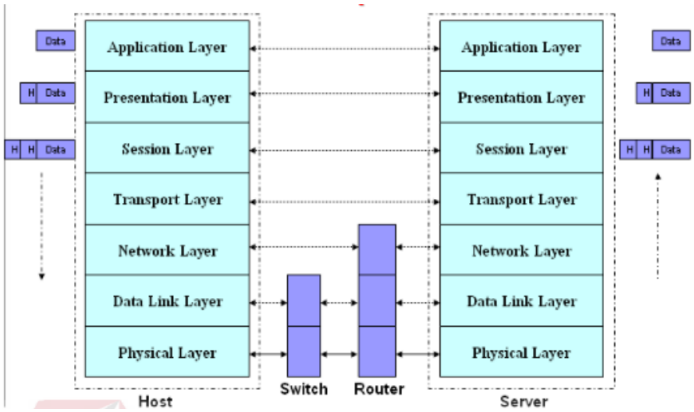
7. *Layer* 7: *Applications*

   Fungsi: Menyediakan komunikasi antar aplikasi.

   Contoh: *Word processing, mail* (*SMTP*). Proses pengiriman data dalam jaringan menggunakan *proses encapsulations*, di mana pesan yang akan dikirim pada *layer Applications* akan dikirim melalui *layer* di bawahnya. Pesan atau data dipotong sesuai dengan ukuran protokol jaringan kemudian ditambahkan *header*. *Link* fisik ada pada *layer* 1. Pada sisi penerima, akan terjadi proses kebalikannya, yang disebut sebagai *decapsulations*[12].

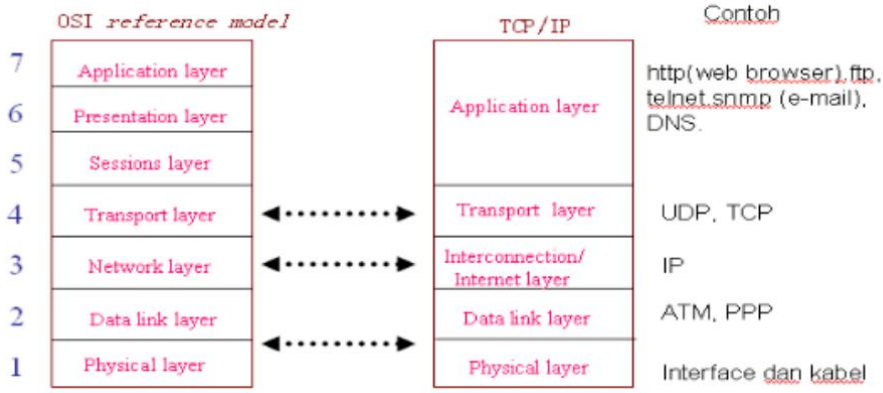
2.2.3 *PROTOCOL TCP/IP*

TCP/IP adalah protokol standar komunikasi data yang digunakan untuk mengirim dan menerima data antara komputer-komputer. *TCP/IP* merupakan jaringan terbuka yang independen terhadap mekanisme transportasi pada jaringan fisik yang digunakan, sehingga dapat digunakan di berbagai lokasi dengan fleksibilitas tinggi. Selain itu, *TCP/IP* juga mendukung interoperabilitas antara berbagai perangkat dan jaringan yang berbeda



Gambar 2.3 *Decapsulation*[12]

Gambar 2.3 merupakan *decapsulation* dari layer osi, fungsi-fungsi dalam *TCP/IP* sesuai dengan fungsi-fungsi yang ada dalam *layer* OSI. Tiga *layer* di atas digabung menjadi satu *layer* yang disebut sebagai *layer* Aplikasi. *Layer* Interkoneksi juga sering disebut sebagai *layer* internet. Beberapa referensi menggabungkan *layer data link* dan *layer physical* yang disebut sebagai *Network Interface Layer*.



Gambar 2.4 *TCP/IP* dan OSI Model Pengalamatan[12]

Hubungan antara Layer OSI dan *TCP/IP* dapat dipahami dengan mengacu pada Gambar 2.4. Pengalamatan jaringan dalam protokol *TCP/IP* memiliki variasi berdasarkan lapisan yang ada dalam *TCP/IP*. Pada lapisan *Transport*, pengalamatan menggunakan *port*. Lapisan *Network* menggunakan IP *address* sebagai pengalamatan. Lapisan *data link* mengandalkan *MAC address* sebagai pengalamatan, sementara pada lapisan *Physical*, pengalamatan dilakukan dengan menggunakan *bits*[12].

2.2.3.1 Cara Kerja *Router*

Router adalah sebuah perangkat fisik atau *virtual* yang didesain untuk menghubungkan, menganalisis, dan mengarahkan paket data di antara jaringan komputer. *Router* memeriksa alamat *IP* tujuan dari paket data yang diterima, menggunakan informasi dalam *header* paket, dan menentukan jalur yang paling efisien untuk meneruskan paket tersebut.

Dengan menganalisis alamat *IP* tujuan dalam *header* paket, *router* membandingkannya dengan tabel *routing* yang ada untuk menentukan rute terbaik untuk paket berikutnya.

Tabel *routing* merupakan daftar petunjuk yang mengarahkan pengiriman data ke tujuan jaringan tertentu. Tabel ini memiliki peraturan yang digunakan untuk menghitung jalur terbaik yang harus diambil oleh data menuju alamat *IP* yang dituju.

Pada dasarnya, *router* sangat mengandalkan tabel *routing* untuk menentukan cara mengirim data dan mengenali asal lalu lintas. Tabel *routing* mengatur jalur bawaan yang digunakan oleh *router*. Ada dua jenis tabel *routing*, *routing statis* dan *dinamis*. Tabel *routing statis* diatur secara manual, sementara tabel *routing dinamis* diperbarui secara otomatis berdasarkan aktivitas jaringan[13].

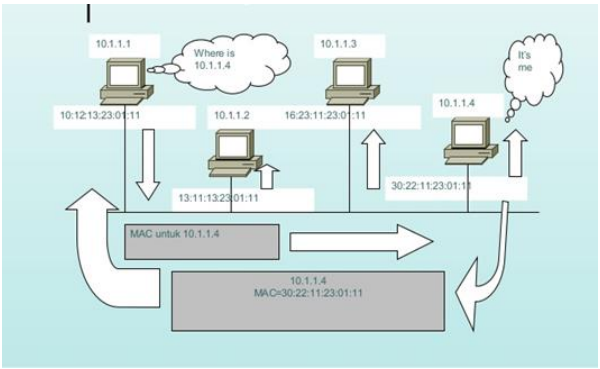
2.2.3.2 Cara Kerja *Switch*

Switching adalah suatu sistem elektronik yang berfungsi sebagai penghubung untuk jalur komunikasi antar perangkat. Jaringan *switching* adalah sebuah infrastruktur yang mampu mengalokasikan sirkuit khusus di antara *node* dan terminal. Ini memungkinkan pengguna untuk berkomunikasi satu sama lain dengan

cara yang efisien dan terdedikasi. *Switch* menyimpan setiap informasi *MAC address* dari setiap perangkat yang terhubung. Dengan informasi ini *switch* bisa mengidentifikasi posisi *port* setiap perangkat. Saat *frame* diterima, *switch* bisa dengan pasti menentukan *port* yang akan digunakan untuk mengirimkan *frame* tersebut.

Setelah perangkat terkoneksi dengan *switch*, *switch* akan merekam alamat *Media Access Control* (*MAC*) perangkat tersebut. Dengan kata lain, alamat *MAC* mengenali perangkat fisik, berbeda dengan alamat IP yang berada di tingkat jaringan (*Layer* 3) dan dapat berubah seiring waktu. Meskipun switch bekerja pada Layer 2, ada juga kemampuan operasi pada *Layer* 3. Ini diperlukan untuk mendukung jaringan lokal *virtual* (*VLAN*), yang memungkinkan segmentasi logis jaringan di dalam satu *subnet*. Agar lalu lintas dapat berpindah antar *subnet*, perlu melewati antar *switch*, dan fitur ini dibantu oleh kemampuan *router* yang terintegrasi dalam *switch*[14].

ARP adalah sebuah protokol yang digunakan untuk mengaitkan alamat *IP* dengan alamat *MAC* (*Media Access Control*). Fungsinya adalah untuk menghubungkan lapisan 2 (*Data Link*) dengan lapisan 3 (*Network*). Keberadaan *ARP* sangat penting karena membantu *router* dalam mengirimkan data dengan lebih efisien, karena alamat yang diperlukan sudah tercatat dalam tabel *ARP*. Dalam rangka melakukan pemetaan alamat *IP* ke alamat *Ethernet* yang terhubung, digunakan protokol *ARP* (*Address Resolution Protocol*). Proses pemetaan ini diperlukan saat datagram dikirimkan ke *host*, karena pada saat itu *host* menambahkan *header Ethernet* pada datagram. Upaya menerjemahkan alamat *IP* ke alamat *Ethernet* ini, untuk mempermudah pengiriman, biasa disebut sebagai tabel *cache*.



Gambar 2. 5 Cara Kerja *ARP*

Gambar 2.5 merupakan cara kerja dari *ARP*, proses *ARP* dalam mengaitkan alamat *IP* dengan alamat *MAC* memiliki langkah-langkah sebagai berikut:

1. Ketika sebuah *host* mengetahui alamat *IP* dari tujuan tetapi tidak memiliki informasi tentang alamat *MAC*-nya, *host* tersebut menginisiasi permintaan *ARP*. Permintaan *ARP* (*ARP request*) mengandung alamat *IP* yang sudah diketahui sebelumnya, dan kemudian permintaan ini disiarkan ke seluruh perangkat dalam jaringan lokal.
2. Pesan broadcast *ARP request* diterima oleh semua perangkat dalam segmen Ethernet. Saat target yang memiliki alamat *IP* yang sesuai membaca isi pesan *ARP request*, ia akan merespons dengan balasan *ARP* (*ARP reply*) secara *unicast* ke pengirim permintaan. Balasan ini berisi alamat *MAC* yang diperlukan.
3. Proses resolusi alamat berhasil ketika pengirim menerima balasan *ARP* dari target yang berisi alamat *MAC* yang sesuai. *Host* pengirim kemudian memperbarui tabel *ARP cache* atau *ARP table*. Tabel ini berfungsi untuk mencatat hubungan antara alamat *IP* dan alamat *MAC* yang cocok.
4. Binding atau asosiasi dalam tabel *ARP cache* tetap disimpan, diperbarui, dan dijaga. Entri dalam tabel ini dapat dihapus setelah melewati periode waktu tanpa aktivitas tertentu. Lama waktu ini bergantung pada sistem operasi yang digunakan.
5. Mekanisme *aging out* digunakan untuk memastikan bahwa tabel *ARP cache* tidak berisi informasi tentang *host* yang mungkin telah dimatikan atau dipindahkan ke tempat lain.

Dengan demikian, proses *ARP* memungkinkan host dalam jaringan untuk memetakan alamat *IP* ke alamat *MAC* yang sesuai, memudahkan komunikasi data di lapisan *Data Link* (*Layer* 2) dalam jaringan *Ethernet*[15].

2.2.4 *LAN*

Local Area Network (*LAN*) merupakan sebuah jaringan komputer yang terbatas pada wilayah lokal tertentu. Dengan demikian, hanya pengguna yang berada dalam area *LAN* tersebut yang dapat mengakses jaringan. Untuk

menghubungkan perangkat ke internet dalam *LAN*, digunakan perangkat-perangkat jaringan sederhana seperti kabel *UTP*, *hub*, *switch*, dan *router*.

Jaringan jenis ini memiliki beberapa karakteristik yang mudah dikenali antara lain:

1. *LAN* tidak bergantung pada jaringan telekomunikasi tambahan dari operator.
2. Jaringan ini umumnya digunakan untuk kepentingan pribadi atau internal tertentu dalam suatu organisasi atau lingkungan tertentu.
3. Administrasi pada jaringan dilakukan secara lokal oleh pihak pengelola di dalam lingkungan tersebut.
4. Pada jaringan *LAN*, seringkali terdapat satu komputer yang berfungsi sebagai server untuk mengatur sistem agar berjalan dengan lancar dan memenuhi kebutuhan para pengguna lainnya dalam lingkungan jaringan tersebut.

Jaringan *Local Area Network* (*LAN*) memiliki beberapa fungsi, di antaranya:

1. Menghubungkan 2 Komputer atau Lebih

   Jenis jaringan komputer ini digunakan untuk menghubungkan dua komputer atau lebih, baik secara langsung ataupun melalui perangkat perantara seperti *switch* atau *hub*. Dua komputer dapat dihubungkan langsung menggunakan kabel UTP yang terpasang pada kedua komputernya. Untuk menghubungkan banyak komputer sekaligus diperlukan perangkat tambahan seperti *switch* atau *hub*. Dengan demikian, jaringan *LAN* memungkinkan komunikasi dan berbagi data di antara komputer-komputer yang terhubung di dalam *area* yang terbatas tersebut.
2. Memindahkan File dari Satu Komputer ke Komputer Lainnya

   Dengan jaringan *LAN*, proses transfer data dari satu komputer ke komputer lainnya menjadi lebih efisien. Tidak lagi perlu menggunakan *flash disk* atau perangkat eksternal lainnya. Dalam jaringan *LAN*, pemindahan *data* dapat dilakukan dengan mudah melalui metode *sharing file*, yang memungkinkan pengguna untuk berbagi dan mengakses file dari berbagai komputer yang terhubung dalam jaringan.
3. *Sharing Printer*

   Salah satu keuntungan jaringan *LAN* adalah kemampuan untuk berbagi *printer*. Dengan menghubungkan printer ke salah satu komputer dalam jaringan,

pengguna dapat membagikan printer tersebut sehingga bisa digunakan bersama oleh semua pengguna dalam jaringan. Langkahnya cukup sederhana, pengguna hanya perlu membagikan driver *printer* yang ada di *Control Panel*, dan setelah itu *printer* dapat digunakan secara bersama-sama tanpa perlu memindahkan komputer atau *printer*. Hal ini tidak hanya memudahkan semua pengguna, tetapi juga membantu menghemat biaya karena satu *printer* dapat digunakan oleh banyak pengguna dalam jaringan.

4. *LAN Chatting*

   Dengan jaringan *LAN*, pengguna dapat melakukan *chatting* atau mengirim pesan antar komputer yang terhubung dalam area jangkauan jaringan. Aktivitas ini dapat dilakukan tanpa harus terhubung ke internet, sehingga memudahkan komunikasi antar pengguna dalam jaringan *LAN* meskipun tidak memiliki akses ke internet. Dengan demikian, jaringan *LAN* tetap dapat digunakan untuk aktivitas chatting atau berkomunikasi secara lokal.

5. *Remote* Komputer

   Aktivitas *remote* pada suatu komputer dapat dilakukan menggunakan perangkat lunak seperti *TeamViewer*, yang memungkinkan pengguna untuk mengakses dan mengontrol komputer dari jarak jauh. Namun demikian, dalam solusi tersebut, komputer yang akan di-*remote* harus terhubung ke internet agar dapat diakses dari lokasi lain[16].

2.2.5 *VLAN*

Virtual local area network (*VLAN*) merupakan sekelompok perangkat dalam jaringan *LAN* yang dikonfigurasi menggunakan perangkat lunak manajemen agar dapat berkomunikasi jika terhubung ke *switch* yang sama dan ditempatkan pada segmen *LAN* yang berbeda. Penggunaan *VLAN* memberikan berbagai keuntungan, termasuk meningkatkan tingkat keamanan dan membagi *domain* menjadi beberapa *broadcast* yang lebih kecil. Hal ini terjadi karena *VLAN* bekerja berdasarkan *logical connection* daripada *physical connection*, sehingga memberikan fleksibilitas yang tinggi dalam mengatur komunikasi antar perangkat dalam jaringan. Dengan demikian, *VLAN* menjadi solusi yang efisien dan aman untuk mengatur dan mengelola jaringan komputer dalam lingkungan *LAN*[17]**.**

Fungsi dari *Virtual Local Area Network* (*VLAN*) dalam jaringan komputer adalah menyediakan metode yang efisien untuk membagi jaringan fisik menjadi beberapa *broadcast domai*n[18]. Dengan adanya *VLAN*, *domain broadcast* tersebut dapat meningkatkan keamanan dan efisiensi jaringan. Meskipun setiap *VLAN* memiliki *domain broadcast* yang berbeda, mereka tetap menggunakan perangkat penghubung yang sama untuk jalur koneksi mereka. Umumnya, konfigurasi *VLAN* dapat dilakukan menggunakan perangkat khusus seperti perangkat MikroTik atau Cisco yang dirancang untuk mengelola jaringan dengan fitur *VLAN* secara efektif.[19].

IEEE melakukan standarisasi beberapa protokol terkait dengan jaringan *LAN*, termasuk protokol *VLAN trunking*. Salah satunya adalah 802.1Q yang menggunakan *header* berbeda dari ISL untuk menyematkan informasi *VLAN* pada *frame*. Sebuah *trunk* adalah koneksi titik-ke-titik antara dua perangkat jaringan yang memungkinkan membawa beberapa *VLAN* secara bersamaan. *Cisco* mendukung penggunaan IEEE 802.1Q untuk mengoordinasikan *trunk* di *interface Fast Ethernet*, *Gigabit Ethernet*, dan 10-*Gigabit Ethernet*.

Penggunaan *VLAN* memungkinkan adanya beberapa jaringan *subnet* yang dapat berbagi satu *switch*. Konfigurasi *VLAN* dilakukan melalui perangkat lunak (*software*), sehingga meskipun komputer berpindah tempat, ia tetap terhubung pada jaringan tersebut. Dengan menggunakan *VLAN*, jaringan dapat di-segmentasi berdasarkan fungsi, departemen, atau tim proyek yang memungkinkan lebih fleksibel dalam mengatur akses dan keamanan dalam suatu jaringan serta dapat diimplementasikan secara efisien dan fleksibel[20].

Produktivitas pengguna dan adaptabilitas jaringan merupakan faktor kunci bagi pertumbuhan bisnis. Dalam hal ini, *VLAN* memberikan kemudahan dalam merancang jaringan yang sesuai dengan tujuan organisasi. Beberapa manfaat utama yang dihadirkan oleh penggunaan *VLAN* adalah sebagai berikut:

1. *Security* (Keamanan)

   Sebuah kelompok data yang sensitif diisolasi dari jaringan lain untuk mengurangi potensi risiko pelanggaran informasi rahasia. Seperti yang terlihat dalam Gambar 2.5, komputer fakultas ditempatkan dalam *VLAN* 10 dan

sepenuhnya terisolasi dari lalu lintas mahasiswa dan guest, sehingga menjaga keamanan *data* yang lebih baik.

2. *Cost Reduction* (pengurangan biaya)

   Menghemat biaya dengan menggunakan *bandwidth* yang sudah ada secara lebih efisien dan menghindari biaya mahal untuk melakukan peningkatan perluasan jaringan.

3. *Better Perfomance* (kinerja yang lebih baik)

   Dengan membagi jaringan *layer* 2 menjadi kelompok *broadcast domain* yang lebih kecil, secara efektif mengurangi jumlah lalu lintas paket yang tidak diperlukan dalam jaringan.

4. Mengurangi *domain broadcast (Shrinking broadcast domains*)

   Dengan membagi jaringan menjadi *VLAN*, jumlah perangkat yang terlibat dalam pembentukan *broadcast storm* dapat dikurangi dengan membatasi *domain broadcast* tersebut. Seperti yang ditunjukkan pada Gambar 2.5, ada enam komputer di jaringan ini tetapi terdapat tiga *domain broadcast* yaitu Fakultas, Mahasiswa, dan *Guest*.

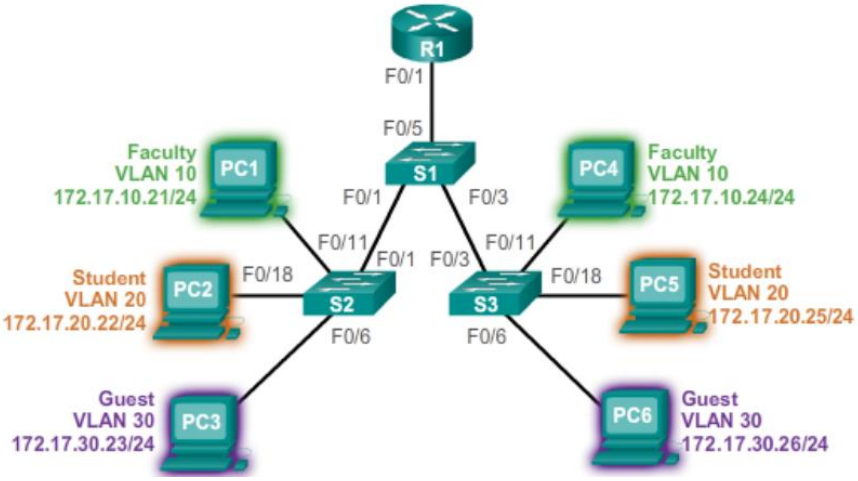
5. Meningkatkan efisiensi staf TI (*Improved IT staff efficiency*)

   Penggunaan *VLAN* mempermudah pengelolaan jaringan karena pengguna dengan kebutuhan sumber daya yang serupa dapat berbagi dalam segmen yang sama. Ketika sebuah *switch* baru diterapkan, semua kebijakan dan prosedur yang telah dikonfigurasi untuk suatu *VLAN* tertentu akan diterapkan saat *port-port* ditugaskan kepada *VLAN* tersebut. Selain itu, hal ini juga memudahkan staf TI untuk mengidentifikasi fungsi dari setiap *VLAN* dengan memberikan nama-nama yang sesuai. Dalam Gambar 2.5, untuk mempermudah pengenalan, *VLAN* dengan nomor urut *VLAN10* dinamai "Fakultas", *VLAN*20 dinamai "Mahasiswa", dan *VLAN*30 dinamai "*Guest*".

6. Manajemen proyek dan aplikasi yang lebih sederhana (*Simpler project* and *application management*):

   VLAN menggabungkan pengguna jaringan dan peralatan untuk mendukung organisasi dan mengatasi kendala geografis; salah satu contoh aplikasinya adalah *platform* pengembangan *e-learning* khusus bagi fakultas.

Dengan membagi jaringan *layer* 2 menjadi kelompok *broadcast domain* yang lebih kecil, secara efektif mengurangi jumlah lalu lintas paket yang tidak diperlukan dalam jaringan.



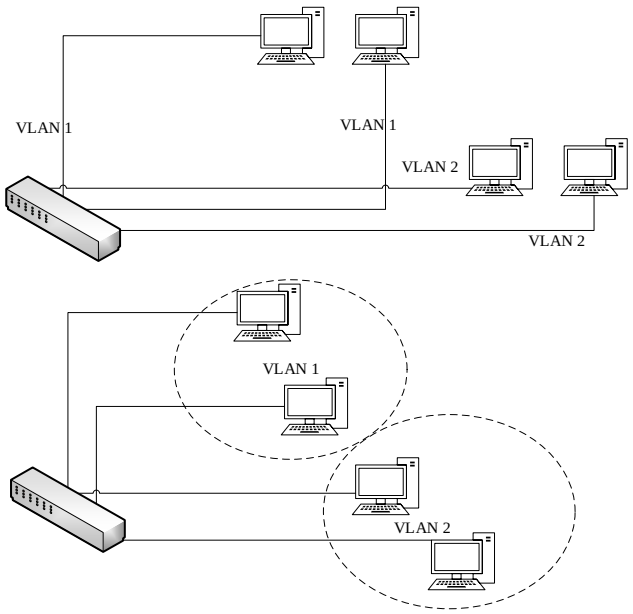
Gambar 2.6 Manfaat *Vlan* [20]

Gambar 2.6 merupakan implementasi dari *vlan*, setiap *VLAN* dalam jaringan diaktifkan sesuai dengan struktur jaringan *IP* yang telah ditetapkan. Oleh karena itu, desain *VLAN* harus mempertimbangkan penerapan skema alamat hirarkis yang sesuai dengan kebutuhan dan tata letak jaringan secara keseluruhan. Pendekatan alamat jaringan hierarkis berarti nomor-nomor jaringan *IP* diberikan secara teratur untuk *segmen-segmen* atau *VLAN-VLAN* tertentu dengan memperhatikan keseluruhan kebutuhan jaringan[20].

Konsep Dasar pada *VLAN*:

1. Membagi satu *domain broadcast* menjadi beberapa *domain broadcast*.
2. Menyediakan keamanan *Layer* 2.
3. Secara *default*, semua *port switch* ditugaskan ke *VLAN* 1.
4. *VLAN* 1 juga dikenal sebagai *VLAN* Administratif atau *VLAN* Manajemen.
5. *VLAN* dapat dibuat dari nomor 2 hingga 1001.
6. Konfigurasi *VLAN* hanya mungkin dilakukan pada *Switch* yang dapat dikelola.
7. Terdapat dua tipe *VLAN*: *VLAN Statis* dan *VLAN* Dinamis.
8. *VLAN* meningkatkan keamanan jaringan.
9. *VLAN* meningkatkan jumlah *domain broadcast* dan mengurangi ukuran *domain broadcast*, yang mengarah pada peningkatan kinerja jaringan[21]

Menerapkan *VLAN* akan memberikan fleksibilitas tinggi dalam konfigurasi jaringan, karena memungkinkan pembuatan segmen-segmen yang sesuai dengan kebutuhan organisasi tanpa harus terkait dengan lokasi *workstation*[22].



Gambar 2.7 Contoh Penggunaan *Vlan*

Gambar 2.7 merupakan pengimplementasikan *VLAN* yang memberikan tingkat fleksibilitas tinggi dalam pengaturan jaringan, karena memungkinkan pembuatan segmen-segmen yang disesuaikan dengan kebutuhan organisasi atau departemen, tanpa harus terikat oleh lokasi kerja seperti yang terlihat pada Gambar 2.7. Terdapat berbagai jenis *VLAN* yang dapat diklasifikasikan berdasarkan *port* yang digunakan, alamat *MAC* (*Media Access Control*), dan tipe protokol yang digunakan[22].

2.2.6 *STP* (*SPANNING TREE PROTOCOL*)

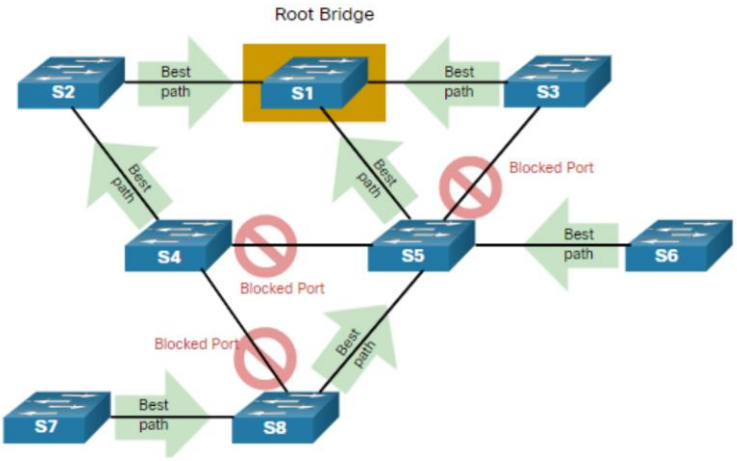
Spanning Tree Protocol (*STP*) merupakan protokol manajemen sistem yang menyediakan jalur-jalur *redundant* sementara untuk mencegah terjadinya masalah *loop* pada jaringan. Salah satu peran penting *STP* adalah mencegah terjadinya *loop* pada *layer* jaringan 2 seperti *bridge* atau *switch*. *STP* secara kontinu memantau jaringan untuk mengidentifikasi semua jalur koneksi dan memastikan bahwa tidak ada *loop* yang terbentuk. Untuk mencapai tujuan ini, *STP* akan menonaktifkan *link*-

link yang bersifat *redundant*, sehingga hanya jalur koneksi yang optimal yang aktif dan digunakan dalam jaringan[23].

Looping dapat menyebabkan ketidakstabilan pada tabel *MAC switch* dan penggunaan *CPU* yang tinggi, sehingga mengakibatkan jaringan tidak dapat berfungsi dengan baik. Adanya redundansi jalur memastikan bahwa layanan jaringan memiliki tingkat kegagalan yang lebih rendah, jika satu jalur mengalami kegagalan, jalur lainnya akan berfungsi sebagai alternatif.

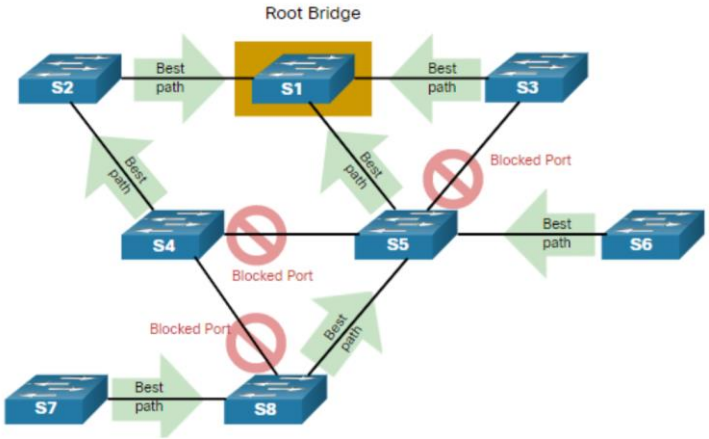
Switch Layer 2 tidak memiliki mekanisme yang serupa dengan *router* untuk membatasi jumlah pengiriman ulang sebuah *frame Layer* 2. Oleh karena itu, ada kebutuhan untuk menggunakan *Spanning Tree Protocol* (*STP*) sebagai langkah pencegahan terhadap masalah *loop* dalam jaringan *Ethernet Layer* 2. Jika *STP* tidak diaktifkan, maka *loop* pada *Layer* 2 dapat menyebabkan *frame broadcast, multicast*, atau *unicast* tanpa alamat tujuan yang dikenal, dan *frame* tersebut akan terus berputar di dalam jaringan, menyebabkan *overhead* yang tidak perlu dan mengganggu kinerja. Hal ini dapat merusak infrastruktur jaringan dengan cepat, terkadang hanya dalam hitungan detik.

STP didasarkan pada algoritma yang dirancang oleh Radia Perlman ketika bekerja di *Digital Equipment Corporation*. Algoritma ini dipublikasikan dalam makalah berjudul "*An Algorithm for Distributed Computation of A Spanning Tree in an Extended LAN*" pada tahun 1985. Algoritma tersebut dikenal sebagai *Spanning Tree Algorithm* (*STA*) yang bertujuan menciptakan topologi jaringan bebas *loop* dengan menetapkan satu *switch* sebagai *root bridge*, sementara *switch* lainnya menentukan *link* dengan biaya paling rendah untuk terhubung ke *root bridge* tersebut[24].



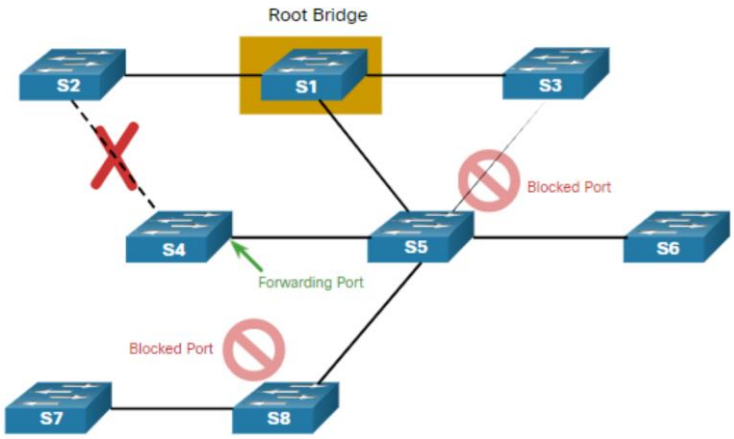
Gambar 2.8 Pemilihan *Root Bridge*[24]

Pada Gambar 2.8, terlihat bahwa *switch* S1 telah menjadi *root bridge* (*bridge* utama) dalam topologi jaringan. Dalam konfigurasi ini, semua *link* memiliki *cost* atau *bandwidth* yang sama. Setiap *switch* menentukan jalur terbaiknya sendiri menuju *root bridge* tersebut. Dalam skenario *STA* dan *STP* ini, istilah "*bridge*" juga digunakan untuk merujuk pada "*switch*", karena pada awal pengembangan *Ethernet*, istilah "*bridge*" digunakan untuk menyebut alat tersebut.



Gambar 2.9 *STP* Memilih Satu Jalur terbaik dan Memblokir Jalur [24]

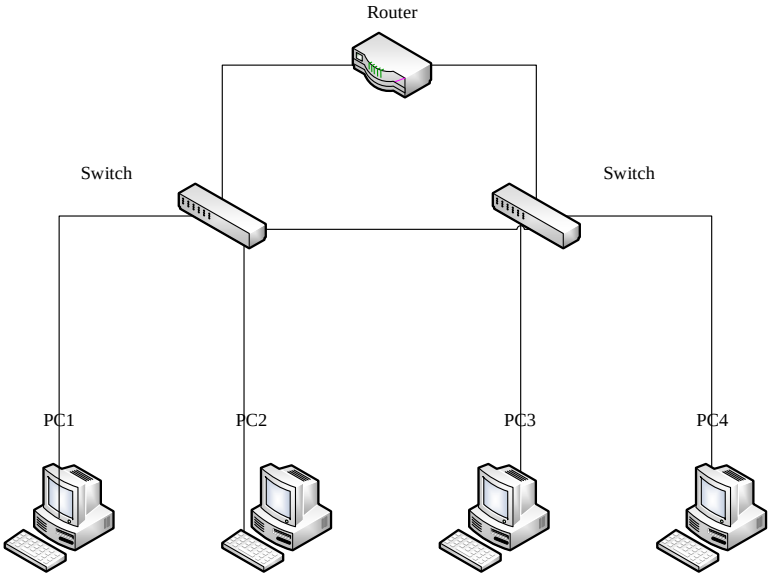
Pada Gambar 2.9, *Switch* S4, S5, dan S8 melakukan pemblokiran pada jalur redundan yang mengarah ke *root bridge* (*bridge* utama). Sebagai hasilnya, setiap *switch* hanya memiliki satu jalur yang terhubung secara logis ke *root bridge* tersebut. *STP* berfungsi untuk mengizinkan hanya satu jalur koneksi yang terhubung secara logis dan akan memblokir semua jalur redundansi untuk mencegah terjadinya perulangan koneksi atau *looping* dalam jaringan.



Gambar 2.10 Kalkulasi Ulang Ketika Ada Kegagalan[24]

Gambar 2.10 mengilustrasikan proses perhitungan ulang oleh *STP* ketika terjadi kegagalan koneksi antara *Switch* (S2) dan *Switch* (S4). Setelah kegagalan tersebut, jalur redundansi sebelumnya antara *Switch* (S4) dan *Switch* (S5), yang sebelumnya diblokir oleh *STP* untuk mencegah perulangan, kini dibuka untuk mengatasi kegagalan tersebut. Meskipun jalur utama mengalami kegagalan, jalur kedua tetap tersedia secara fisik. *STP* akan melakukan perhitungan ulang dan membuka kembali *port* yang sebelumnya diblokir jika terjadi kegagalan pada jalur utama. Perhitungan ulang juga terjadi ketika ada penambahan *switch* atau perubahan dalam topologi. *STP* secara dinamis menyesuaikan diri dengan kegagalan koneksi dengan membuka *port* yang sebelumnya diblokir dan memperbolehkan trafik data pada *port* tersebut. [24].

Dalam protokol *Spanning Tree* terdapat istilah "*Root Bridge" dan "Non-Root Bridge". "Root Bridge" dipilih b*erdasarkan nilai prioritas terendah. Jika nilai prioritas antara dua *switch* sama, maka "*Root-Bridge" akan* ditentukan berdasarkan alamat *MAC* yang lebih kecil di antara kedua *switch* tersebut [25].



Gambar 2.11 Topologi Jaringan *STP*

Gambar 2.11 menunjukkan contoh topologi sederhana dari protokol *Spanning Tree* yang umum digunakan di perusahaan-perusahaan kecil hingga menengah. Topologi tersebut biasanya cukup sederhana dalam implementasinya. Namun, pada perusahaan-perusahaan besar, seringkali digunakan jalur redundan atau koneksi tambahan sebagai cadangan[26].

Protokol *Spanning Tree* (*STP*) beroperasi secara otomatis untuk mengidentifikasi topologi jaringan dan membentuk jalur tunggal yang optimal melalui suatu *bridge* jaringan dengan mengatur fungsi-fungsi pada setiap *bridge*. Fungsi-fungsi pada *bridge* tersebut menentukan cara kerjanya dalam berhubungan dengan *bridge* lainnya, termasuk keputusan apakah akan meneruskan lalu lintas *data* ke jaringan lain atau tidak.[27].

A. Root Bridge

Root Bridge memiliki peran sebagai *bridge* utama atau pengendali dalam sebuah jaringan. Secara periodik, *Root Bridge* mengirimkan pesan konfigurasi yang digunakan untuk memilih rute dan menyesuaikan fungsi-fungsi dari *bridge-bridge* lainnya jika diperlukan. Setiap jaringan hanya memiliki satu buah *root bridge* yang ditentukan oleh administrator berdasarkan kedekatannya dengan titik pusat fisik jaringan tersebut[27].

B. Design Bridge

Designated Bridge merupakan *bridge* tambahan yang bertugas untuk meneruskan paket-paket melalui jaringan. *Bridge* tambahan ini dipilih secara otomatis melalui pertukaran paket konfigurasi *bridge*. Untuk menghindari terjadinya *loop* penyeberangan (*bridging loop*), setiap segmen jaringan hanya memiliki satu *Designated Bridge* saja[27].

C. Backup Bridge

Semua *bridge redundan* dianggap sebagai *bridge* cadangan (*Backup*). *Backup bridge* ini mendengarkan lalu lintas jaringan dan membangun basis *data bridge* tanpa meneruskan paket-paket tersebut. Jika terjadi kegagalan pada *Root Bridge* atau *Designated Bridges*, maka fungsi-fungsi tersebut akan diambil alih oleh *bridge* cadangan ini. Setiap *bridge* mengirimkan paket khusus yang dikenal sebagai *Bridge Protocol Data Unit*s (BPDU) melalui setiap *port*nya.

Pentingnya pengiriman dan penerimaan BPDU dari berbagai *bridge lain* adalah untuk menentukan fungsi-fungsi dari masing-masing *bridge*, melakukan verifikasi apakah ada perubahan status fungsionalitas pada sekitarannya, serta melakukan pemulihan jika terjadi perubahan topologi dalam sebuah jaringan.

Perencanaan konfigurasi yang melibatkan penggunaan berbagai jenis *bridge* dengan protokol *Spanning Tree* memerlukan perhatian yang teliti. Untuk mencapai konfigurasi yang optimal, peraturan-peraturan berikut harus diperhatikan dengan cermat:

a) Setiap *bridge* sebaiknya memiliki cadangan jalur (yaitu jalur redundan antara setiap *segmen*).
b) Paket-paket dalam jaringan sebaiknya tidak melewati lebih dari dua *bridge* antara segmen-segmen jaringan.
c) Setelah terjadi perubahan dalam topologi jaringan, paket-paket sebaiknya tidak melewati lebih dari tiga *bridge*[27].

2.2.7 KEAMANAN JARINGAN

Keamanan jaringan komputer merupakan upaya untuk mencegah dan mendeteksi penggunaan yang tidak sah dalam sebuah jaringan komputer. Tujuan dari keamanan jaringan komputer adalah untuk mengidentifikasi dan mengatasi

potensi risiko yang dapat terjadi pada jaringan tersebut baik dalam bentuk ancaman fisik maupun logikal yang dapat mengganggu aktivitas-aktivitas yang berlangsung di dalamnya secara langsung atau pun tidak langsung. Selain itu, tujuan lainnya adalah menjaga keamanan data-*data* yang tersimpan dalam sistem komputer agar tetap aman dari berbagai macam ancaman yang ada[28]**.**

Konsep keamanan jaringan:

1. Kerahasiaan (*Confidentiality*):

   Kerahasiaan bertujuan untuk melindungi informasi sensitif dan membatasi akses hanya kepada pihak yang berwenang melalui pelatihan khusus jika diperlukan.

2. Integritas (*Integrity*):

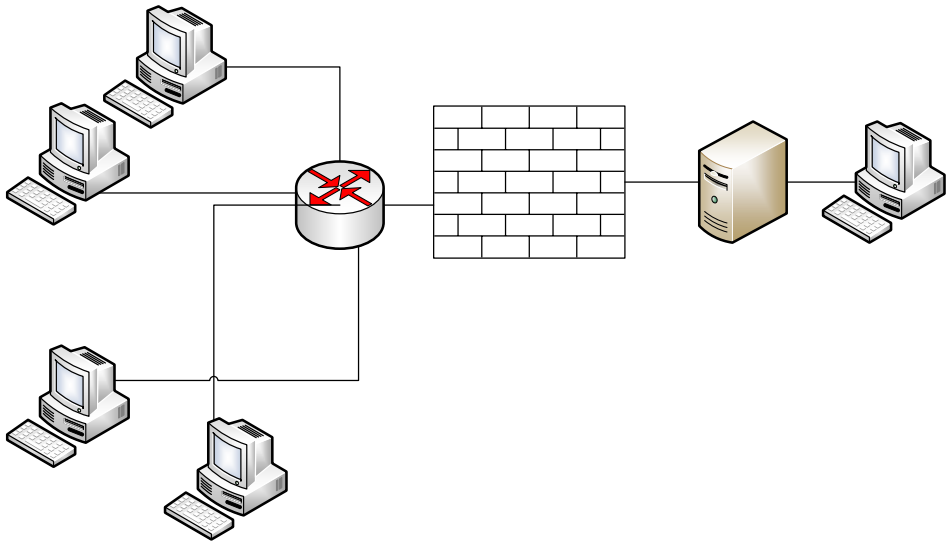
   Integritas menjamin keberlanjutan konsistensi dan akurasi data dengan mencegah perubahan oleh pihak yang tidak berwenang.

3. Ketersediaan (*Availability*):

   Ketersediaan mencakup pemeliharaan optimal komponen perangkat keras serta penanganannya dengan cepat saat terjadi kerusakan. Selain itu, ketersediaan juga melibatkan pemeliharaan lingkungan operasional sistem yang stabi[29].

2.2.8 *FIREWALL*

Next-Generation Firewall (*NGFW*) merupakan evolusi dari teknologi firewall generasi ketiga yang dapat diimplementasikan dalam bentuk perangkat lunak atau perangkat keras. *NGFW* memiliki kemampuan canggih untuk mendeteksi dan menghalangi serangan *cyber* dengan tingkat perlindungan yang tinggi, termasuk penerapan keamanan pada level protokol, *port*, dan aplikasi. Keunggulan *NGFW* terletak pada kemampuannya untuk menyederhanakan kompleksitas dengan memberikan visibilitas otomatis terhadap penggunaan aplikasi-aplikasi tertentu. Pengguna-pengguna dan jaringan akan dapat bekerja secara aman bersama-sama sehingga menciptakan hasil kinerja yang optimal[30]**.**



Gambar 2.12 *Firewall* Sebagai Pos Keamanan Jaringan

Gambar 2.12 menunjukkan bahwa *Firewall* merupakan pos keamanan jaringan dengan beberapa poin penting yang menjelaskan fungsi-fungsi penting untuk melindungi jaringan komputer adalah sebagai berikut:

1. Sebagai Pos Keamanan Jaringan: Seluruh lalu lintas masuk dan keluar jaringan harus melewati *firewall* sebagai pos keamananan yang melakukan pemeriksaannya. Setiap ada lalu lintas, *firewall* akan berusaha menyaring agar sesuai dengan tingkat keamanannya.
2. Melindungi informasi berharga dari bocor tanpa izin adalah tujuan utama dari fungsi ini. Untuk mencapai hal tersebut, sering kali digunakan *firewall* yang khusus didesain untuk mengatur aliran *data* pada protokol *File Transfer Protocol* (*FTP*). *Firewall* berguna dalam mencegah pengguna di dalam jaringan mengirimkan file-file bernilai tinggi yang bersifat rahasia kepada orang lain tanpa izin.
3. Mencatat Aktivitas Pengguna: Setiap kali pengguna berupaya untuk mengakses data, mereka harus melalui *firewall* terlebih dahulu dan aktivitas tersebut dicatat sebagai dokumentasi (*filelog*) yang nantinya bisa digunakan untuk meningkatkan keamanan sistem. *Firewall* mampu mengakses *data log* sekaligus memberikan statistik tentang penggunaan jaringan.[31].

2.2.9 *ACCESS CONTROL LIST*(*ACL*)

ACL (*Access Control List*) adalah fitur keamanan pada *router Cisco* yang berfungsi untuk memilih paket-paket data yang masuk atau keluar dari *router* berdasarkan serangkaian aturan. *ACL* menentukan apakah paket-paket tersebut diizinkan (*permit*) atau ditolak (*deny*)[32]**.**

Untuk memfilter lalu lintas jaringannya sendiri, Pada *interface router* yang digunakan, *Access Control List* (*ACL*) digunakan untuk memutuskan apakah paket tersebut harus diteruskan atau diblokir. *Router* menggunakan berbagai informasi seperti alamat sumber dan tujuan, protokol, dan nomor *port* untuk melakukan pengambilan keputusan tersebut. Untuk mengontrol arus lalu lintas yang masuk dan keluar dari sebuah jaringan, setiap protokol pada setiap *interface* harus diatur dengan baik dan didefinisikan secara tepat. Untuk mengatur arah *trafik* di dalam sebuah jaringan, dua buah jenis *list* terpisah harus dibuat yaitu satu untuk mengontrol *trafik* yang masuk dan satu lagi untuk mengontrol *trafik* yang keluar.

Berikut adalah beberapa fungsi penting dari penggunaan *Access Control List* (*ACL*):

1) Membatasi jumlah lalu lintas pada jaringan serta meningkatkan kinerja keseluruhan jaringan. Sebagai contoh, *ACL* dapat memblokir lalu lintas video sehingga mengurangi beban jaringan dan meningkatkan kinerja keseluruhan.
2) Mengatur aliran lalu lintas dengan baik. Misalnya, *ACL* mampu memblokir *update routing* yang tidak diperlukan dan dengan demikian membantu menghemat *bandwidth*.
3) Menyediakan kontrol akses ke dalam sebuah jaringan. Sebagai contoh, *host* A diberi akses terbatas ke jaringan sementara *host* B diizinkan penuh.
4) Menentukan lalu lintas jenis apa yang diperbolehkan atau diblokir melalui *interface router*. Misalnya, lalu lintas email diizinkan sementara lalu lintas telnet diblokir.
5) Mengelola *area-area* di mana klien diizinkan mengakses jaringan.
6) Memilih host-host tertentu yang diizinkan atau dilarang mengakses *segmen-segmen* dalam jaringan. Sebagai contoh, *ACL* dapat mengizinkan atau memblokir akses *FTP* atau *HTTP* [20].

Jenis-jenis *ACL*:

1. *Standard ACL*

   Standard ACL menggunakan hanya alamat *IP* sumber dalam paket *IP* sebagai kondisi yang diuji. Semua keputusan dibuat berdasarkan alamat *IP* sumber tersebut. Dengan demikian, *standard ACL* secara keseluruhan memungkinkan atau memblokir seluruh paket protokol tanpa membedakan jenis lalu lintas *IP* seperti WWW, telnet, UDP, atau DSP.

   Standard ACL melakukan pemeriksaan terhadap alamat sumber pada paket-paket *IP* yang diroutingkan. Berdasarkan perbandingan tersebut, *ACL* akan menentukan apakah akses diizinkan atau ditolak untuk semua lalu lintas protokol, tergantung pada pengaturan jaringan, subnet, dan alamat *host*. Sebagai contoh, ketika paket-paket masuk melalui *interface* Fa0/0, *ACL* akan memeriksa alamat sumber dan protokolnya untuk mengambil keputusan mengenai akses yang diizinkan atau ditolak. Jika sebuah paket diperbolehkan, maka akan dirouting melalui *router* menuju *interface* keluarannya. Namun jika sebuah paket tidak diperbolehkan maka akan dihentikan saat tiba di *interface* masukannya. Untuk membuat *Standard ACL* dapat digunakan perintah konfigurasi *global access-list* dengan angka 1 hingga 99[20].

   Perintah lengkap standar *ACL* adalah:

   Router(*config*)# *access-list access-list-number deny —permit source* [*source-wildcard*] [*log*]

   Untuk menghapus *ACL*, Anda dapat menggunakan perintah "*no*" sebelum perintah *ACL*, seperti contoh:

   Router(*config*)# no *access-list access-list-number*[20].

   Ciri dari *ACL Standard*:

   1. Range nomor: 1-99.
   2. Digunakan untuk menyaring alamat *IP* sumber.
   3. Mengizinkan atau menolak semua protokol *suite TCP/IP*[21]

2. *Extended Access Control List* (*ACL*)

   Extended ACL adalah jenis daftar kontrol akses yang menyediakan tingkat keamanan yang lebih tinggi daripada *Standard ACL*. *Extended ACL*

diterapkan pada *router* sumber dan memungkinkan izin atau penolakan paket berdasarkan alamat sumber dan tujuan secara bersamaan. Dengan menggunakan *Extended ACL*, *administrator* jaringan memiliki fleksibilitas yang lebih besar dalam melakukan proses penyaringan dengan tujuan yang lebih spesifik[7].

Penerapan daftar *Extended Access List* (*ACL*) pada *router* berfungsi sebagai mekanisme penyaringan pertama dalam jalur komunikasi data di dalam jaringan. Tugasnya sangat penting karena bertujuan untuk mengatur dan mengontrol semua aktivitas informasi yang masuk dan keluar dari jaringan. Dengan adanya *ACL*, *router* dapat mendeteksi dan mencegah ancaman potensial yang berasal dari pihak eksternal yang mencoba untuk memanfaatkan atau menyalahgunakan paket-paket *data* dalam jaringan. Dengan demikian, *ACL* berperan sebagai lapisan pertama pertahanan dalam menjaga keamanan dan integritas jaringan dari ancaman-ancaman yang berpotensi merugikan[8].

Daftar Kontrol *Extended Access List* memiliki kemampuan untuk mengevaluasi beberapa *field* lainnya pada *header layer* 3 dan *layer* 4 dari paket-paket IP. Hal ini termasuk kemampuan untuk menilai alamat *IP* sumber dan tujuan, bidang protokol dalam *header layer* jaringan, serta nomor *port* pada *header layer transport*. Dengan fitur ini, *Extended ACL* dapat membuat keputusan yang lebih spesifik saat mengontrol lalu lintas di jaringan.

Konsep yang dimiliki oleh *Extended Access Control List* adalah kemampuannya untuk melakukan penyaringan berdasarkan alamat sumber dan tujuan secara lebih spesifik, memberikan kemudahan bagi operator jaringan dalam menjalankan proses penyaringan dengan tujuan yang lebih tepat[33].

Daftar kontrol *Extended access list* mencocokkan paket dengan memeriksa lalu lintas asal dan tujuannya. Tidak seperti daftar kontrol akses standar yang hanya mempertimbangkan lalu lintas asalnya saja. Selain itu, daftar kontrol akses *Extended* juga dapat melakukan penyaringan lalu lintas berdasarkan protokolnya, misalnya hanya menolak lalu lintas protokol *ICMP* atau mengizinkan lalu lintas *HTTP* untuk *host* tertentu saja.

Daftar kontrol *Extended ACL* lebih sering digunakan daripada *ACL* standar karena memberikan rentang kontrol yang lebih luas. Daftar kontrol

akses *Extended* memverifikasi alamat sumber dan tujuan paket, serta memiliki kemampuan untuk memeriksa protokol dan nomor *port*.

Untuk menghubungkan daftar kontrol *Extended ACL* yang sudah ada dengan sebuah *interface*, digunakan perintah "*ip access-group*". Perlu diingat bahwa hanya satu *ACL* yang diizinkan untuk setiap *interface*, tujuan, dan protokol tertentu. Format dari perintah ini adalah:

Router(*config-if*)# *ip access-group access-list-number in — out* 17]

Ciri dari *ACL Extended*:

1. Nomor: 100-199
2. Digunakan untuk menyaring alamat *IP* sumber dan tujuan
3. Dapat melakukan penyaringan berdasarkan *protocol IP* dan nomor *port* secara spesifik[21].

2.2.10 *QUALITY OF SERVICE* (*QOS*)

Quality of Service (*QoS*) didefinisikan sebagai ukuran seberapa baik jaringan dan upaya untuk mendefinisikan karakteristik dan sifat layanan. *IP* mengacu pada kinerja paket *Package IP* yang melewati satu atau lebih jaringan. *Qos* dirancang untuk membantu *end user* menjadi lebih produktif dengan memastikan bahwa *end* user mendapatkan kinerja aplikasi berbasis jaringan yang handal. *Qos* mengacu pada kemampuan jaringan untuk memberikan layanan yang lebih baik pada lalu lintas jaringan tertentu melalui berbagai teknologi. Fitur *Qos* dapat membuat *bandwidth*, latensi dan jitter diprediksi dan disesuaikan dengan kebutuhan aplikasi di jaringan yang ada, oleh karena itu *Qos* sering dijadikan parameter pembanding antara suatu jaringan komputer dan jaringan komputer lainnya[34].

1. *Throughput*

   Throughput merujuk pada kecepatan transfer data yang efektif, diukur dalam *bps* (bit per detik). Ini mewakili total jumlah paket yang berhasil diterima yang diamati di tujuan selama interval waktu tertentu, dibagi oleh durasi *interval* waktu tersebut[35]. *Throughput* dapat dihitung menggunakan persamaan berikut:

$$Throughput = \frac{\text{paket data diterima (bit)}}{\text{waktu pengiriman paket (bit)}} = bps \qquad (2.1)$$

   Tabel 2.2 merupakan tabel kategori *throughput* menurut standar *TIPHON*[36].

Tabel 2.2 *Throughput*

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

2. *Packet Loss*

Ini adalah suatu parameter yang mengindikasikan suatu situasi dimana jumlah keseluruhan paket yang hilang dapat disebabkan oleh tabrakan (*collision*) dan kepadatan (*congestion*) dalam jaringan [35]. Perhitungan *Packet Loss* dapat dilakukan menggunakan persamaan berikut:

$$Packet\ Loss = \frac{(\text{paket data dikirim} - \text{paket data diterima})\text{x}100\%}{\text{paket data dikirim}} = \% \qquad (2.2)$$

Tabel 2.3 merupakan tabel kategori *Packet Loss* menurut standar *TIPHON*[36].

Tabel 2.3 *Packet Loss*

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