BAB II
DASAR TEORI

2.1 TINJAUAN PUSTAKA

Pada tabel 2.1 merupakan tabel perbandingan penelitian terdahulu dan penelitian sekarang:

Tabel 2.1 Penelitian Terdahulu

No	Nama peneiti	Judul Penelitian	ACL	*Cisco Packet Tracer*/GNS3	VLAN	QoS
1	Umar Hasan, Sari Dewi, Firmansyah. 2022	Penerapan Metode *Access Control List* Pada Jaringan VLAN Menggunakan Router Cisco	Ya	*Cisco Packet Tracer*	Ya	Tidak
2	Ahmad Fitriansyah, Alarik Andreansyah dan Abu Sopian. 2019	penerapan statik VLAN dan *Access List* untuk meningkatkan keamanan jaringan studi kasus PT. Dimensi Mandiri teknologi	Ya	*Cisco Packet Tracer*	Ya	Tidak
3	Agung Tri Laksono, M. Alvian Habib Nasution. 2020	Implementasi Keamanan Jaringan Komputer *Local Area Network* Menggunakan *Access Control List* pada Perusahaan X	Ya	*Cisco Packet Tracer*	Tidak	Tidak
4	Nanda Gusti Arirapha	Analisis Penerapan *Acces Control List* (ACL) Sebagai Pembatasan Hak Akses Pada Jaringan Berbasis Vlan Trunking Protocol (VTP)	Ya	GNS3	Ya	Ya

Penelitian Umar Hasan, Sari Dewi, Firmansyah, 1 Januari 2022 yang berjudul "Penerapan Metode *Access Control List* Pada Jaringan VLAN Menggunakan *Router* Cisco". Tujuan dari penulisan ini yaitu untuk membatasi beberapa PC *client* untuk melakukan *transfer* file terhadap server dengan menggunakan metode *access list.*. hasil penelitian yang didapat adalah saat ketika PC *client* yang sudah terdaftar dalam *access list* dengan perintah *deny* ketika akan mencoba melakukan *file transfer protocol*

maka akan terjadi penolakan oleh adanya *access list*[5].

Selanjutnya penelitian Ahmad Fitriansyah, Alarik Andreansyah dan Abu Sopian pada 2 september 2019 yang berjudul "penerapan statik VLAN dan *Access List* untuk meningkatkan keamanan jaringan studi kasus PT. Dimensi Mandiri teknologi". Penelitian ini memaparkan tentang kombinasi antara *Access List* dan *firewall router* sebagai kemanan dalam jaringan komuter dengan menggunakan *Cisco Packet Tracer*. Pada penelitian ini penulis melakukan pengujian dari *access list* dengan tes koneksi antara *client* yang diizinkan atau tidak untuk terhubung terhadap jaringan lainya, pengujian selanjutnya yaitu pengujian dari penerapan *firewall router* yang berfungsi sebagai pemblokiran situs-situs yang tidak bisa diakses *client*[6].

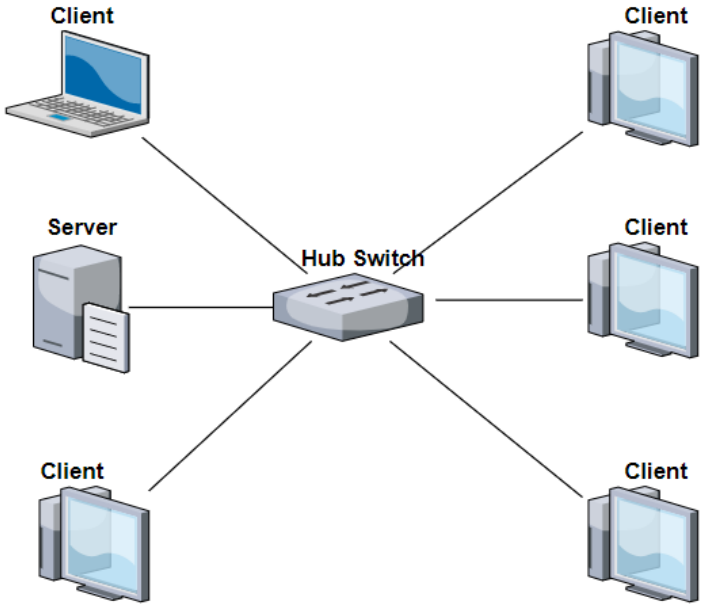
Penelitian selanjutnya yang dilakukan oleh Agung Tri Laksono dan M. Alvian Habib Nasution pada Januari 2020 yang berjudul Implementasi Keamanan Jaringan Komputer *Local Area Network* Menggunakan *Access Control List* pada Perusahaan X. Pada penilitianya pennulis bertujuan untuk mengamankan server dari *client* yang tidak memiliki akses untuk melakukan FTP dan TPFT. Penelitian dilakukan dengan menggunakan sebuah simulator *Cisco Packet Tracer* dengan menggunakan VLAN untuk memanagemen IP *Address*, dari hasil penlitian server yang berada pada gedung 1, 2 dan 3 akan diizinkan untuk mengakses sebuah server pada perusahaan X maka akan memiliki izin tersebut begitu juga sebaliknya. Ketika *client* lain ingin menggunakan servis ftp pada perusahaan X maka akes akan diblokir atau dibatasi. Tujuan dari penelitian ini untuk membatasi transfer file pada perusahaan X yang dapat merugikan perusahaan[4].

2.2 DASAR TEORI

Pada penulisan penelitian ini penulis membutuhkan beberapa teori yang mendukung dalam pelaksanaan penelitian.penulis mengambil isi dari berbagai referensi, seperti buku, *website*, jurnal maupun skripsi. Pada dasar teori ini penulis akan memaparkan tentang jaringan komputer, *switching*, jaringan VLAN, *Access Control List* (ACL), dan beberapa *software* yang digunakan sebagai simulasi ataupun untuk pendukung yang lainya.

2.2.1 Jaringan Komputer

Jaringan komputer merupakan sekumpulan perangkat keras komputer yang saling terhubung satu sama lain sehingga dapat membentuk koneksi dengan menggunakan kabel (*wired*) ataupun tanpa kabel (*wireless*). Jaringan komputer dapat dikatakan terkoneksi apabila komputer satu sama lain dapat saling tehubung dan dapat melakukan pengiriman, penerimaan dan pertukaran data baik dalam bentuk file, suara ataupun gambar yang dapat di terima hingga ketujuan dengan benar[7]. Pada gambar 2.1 merupakan ilustrasi jaringan komputer agar dapat terhubung satu sama lain.



Gambar 2.1 Ilustrasi jaringan komputer[8]

Jaringan komputer memiliki protokol dan algoritma agar bagaiamana data yang dikirim dan diterima dapat tersampaikan dengan tepat sampai tujuanya dan masing-masing komputer berfungsi sebagai *workstation*.yaitu salah satu komputer berfungsi sebagai media jasa atau server terhadap kamputer-komputer yang lainya. Jaringan komputer dapat dibedakan berdasarkan luas wilayang yang ada, berikut adalah pembagian jenis jaringan komputer:[9].

1. *Local Area Network* (LAN)

LAN merupakan singkatan dari *Local Area Network* ini dapat digunakan pada jaringan dengan cakupan wilayah dengan skala kecil saja.

Contohnya hal yang biasa digunakan pada jenis jaringan LAN yaitu perusahaan, sekolah, kampus maupun area lainnya yang memiliki cakupan wilayah yang kecil. Dengan menggunakan LAN, memungkinkan terjadinya beberapa komputer dalam satu wilayah tersebut dapat terhubung satu sama lain sehingga perangkat dalam jaringan LAN dapat bertukar data dan berkomunikasi.

2. *Metropolitan Area Network* (MAN)

Pada jenis jaringan ini MAN dapat digunakan pada luas area sekitar 10 KM sampai dengan 50 KM. Cakupan dari area yang digunakan oleh jaringan MAN ini terbilang cukup luas. MAN merupakan jaringan yang mampu menggabungkan beberapa jaringan LAN yang akan membentuk sebuah jaringan yang lebih luas lagi, maka dari itu jaringan MAN ini sangat cocok untuk digunakan pada jaringan di sebuah pemerintahan pusat dalam suatu kota.

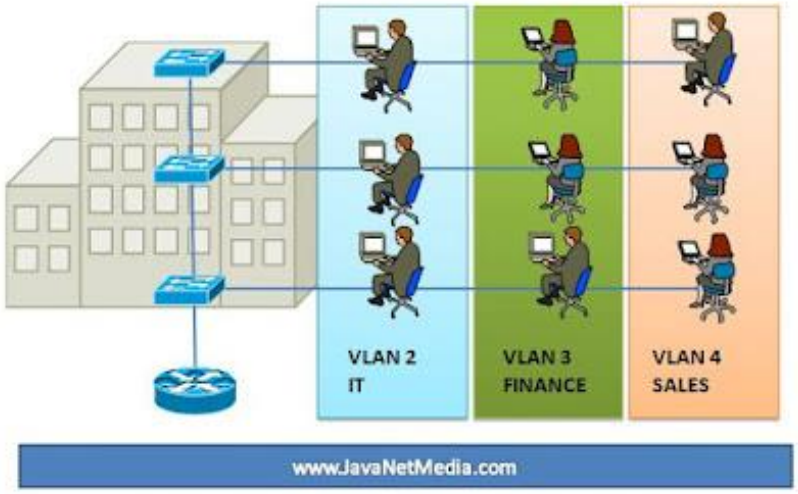
3. *Wide Area Network* (WAN)

Jenis jaringan WAN ini memiliki cakupan wilayah atau jarak yang sangat luas karena jaringan WAN ini mampu menjangkau hingga seluruh negara maupun dunia. Pada jaringan WAN ini biasanya telah terdiri dari jenis jaringan seperti LAN dan MAN. Jenis jaringan WAN ini hanya membutuhkan suatu router saja untuk menghubungkan seluruh komputer ke dalam jaringan. Biasanya WAN dibangun oleh perusahaan *Internet Service Provider* (ISP).

2.2.2 *Virtual Local Area Network* (VLAN)

Virtual Local Area Network (VLAN) atau *logical* LAN atau *logical subnet*, merupakan sebuah metode atau cara untuk memecah *network* menjadi beberapa bagian *network* (*segment*) yang lebih kecil serta dapat dikelompokan dalam satu perangkat ataupun beberapa perangkat yang berbeda dan dapat berkomunikasi satu sama lain seolah-olah VLAN tersebut berada dalam area yang sama. Kegunaan vlan sendiri untuk meminimalisir terjadinya konflik IP yang terlalu banyak, mencegahterjadinya bentrok antar domain (*collision* domain) dan

mengurangi *vulnerabilities*[10]. Ilustrasi penerapan vlan dapat dilihat pada gambar 2.2.



Gambar 2.2 Ilustrasi Penerapan VLAN[11]

VLAN sendiri memiliki macam-macam jenis yang memiliki perbedaan tersendiri, berikut adalah jenis-jenis vlan[12]:

1. Protokol *Routing*
   a. *Inter-Switch Link* (ISL)

   Sebelum IEEE menciptakan dan ditetapkannya standar 802.1Q yang digunakan untuk protokol VLAN trunking cisco menciptakan beberapa tahun terdahulu ISL, karena ISL merupakan hak milik dari cisco maka ISL hanya digunakan untuk antar switch yang hanya mendukung ISL dengan cara kerja membungkus (enkapsulasi) keseluruhan *frame ethernet* dengan ISL *header* dan *trailer* dengan tetap mempertahankan *frame ethernet* original dalam ISL.

   b. IEEE 802.1Q

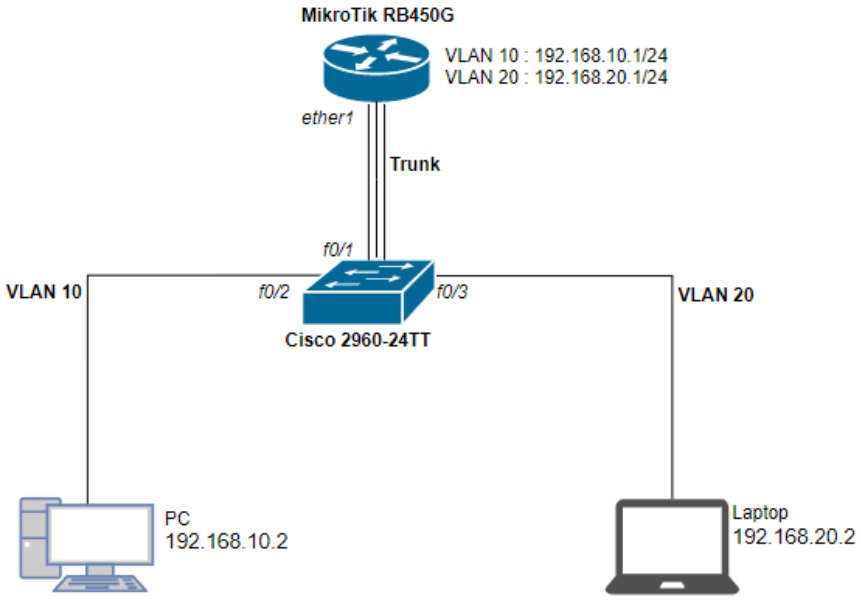
   Institute of Electrical and Electronic Engineering (IEEE) kemudian melakukan standarisasi protokol-protokol yang berkaitan dengan LAN, termasuk protokol VLAN *trunking*. Protokol 802.1Q menggunakan *header* yang berbedan dengan ISL untuk menyematkan angka padan *frame* VLAN. Berbeda dengan ISL 802.1Q tidak melakukan enkapsulasi secara penuh dan sebagai gantinya 802.1Q menyisipkan 4

byte VLAN *header* original dari *frame ethernet.* Hasil yang didapat dari protokol 802.1Q masih memiliki *source* dan *destination* MAC *address* original dan karena pada *header* berbeda maka proses enkapsulasinya menghitung ulang *frame checck sequence* (FCS) asli yang berada pada *ethernet trailer.*

Sedangkan berdasarkan tipe koneksinya VLAN memilik berbagai jenis port yang dibagi atas 3 jenis yaitu:

a. *Trunk Link*

Merupakan sebuah *port* yang dikonfigurasi untuk dapat dilewati beberapa VLAN sekaligus. *Trunk link* mampu menghubungkan *switch* dengan *switch*, *switch* dengan router ataupun *switch* dengan router di mana *trunk link* dapat digunakan untuk melewatkan data dari vlan-vlan yang berbeda. Agar dapat membedakan satu vlan dengan yang launya perlu *trunk link* harus diberi vlan *taging*.

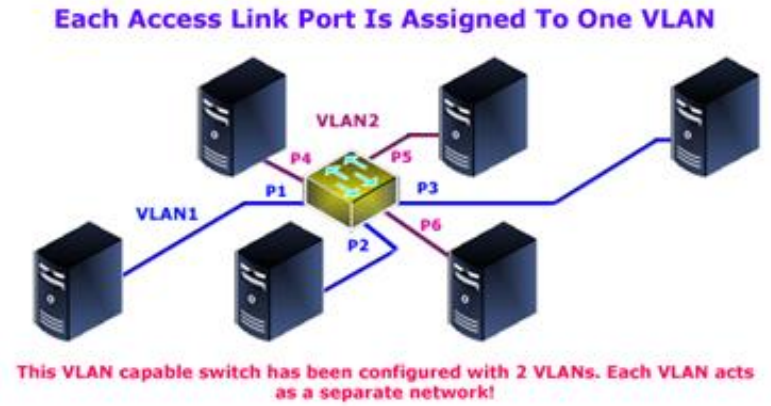


Gambar 2.3 Penerapan *Port Trunk* Pada Perangkat[13]

Trunk link ini dapat juga dikatakan satu kabel fisik yang dapat membawa beberapa vlan dengan adanya trunk link ini upaya penghematan kabel juga dapat dilakukan. Penerapan *port trunk* dapat dilihat pada gambar 2.3.

b. *Access Link*

Access link merupakan sebuah *port* yang dapat dikonfigurasi dan dikhususkan untuk dilewati satu vlan saja. Pada umumnya *access link* dikhususkan untuk menghubungkan *switch* dengan *end-device* seperti komputer, *printer*, cctv dan yang lainya. Adapun penerapan dari *acces link* terdapat pada gambarh 2.4.



Gambar 2.4 penerapan *access port* pada perangkat[14]

c. *Hybrid Link*

Hybrid Link merupakan sebuah *port* yang dikonfigurasi dengan menggabungkan antara *trunk link* dan *access link*, *hybrid link* mampu menjalankan *trunk link* dan *access link* secara bersamaan.

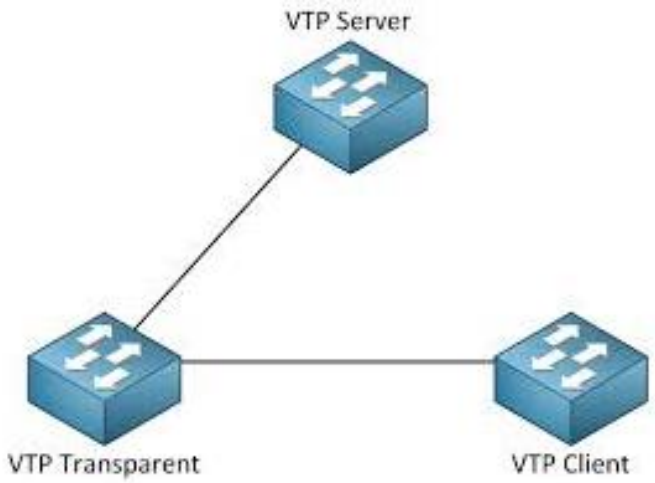
2.2.3 VLAN *Trunking Protocol* (VTP)

VLAN *Trunking Protocol* merupakan protokol yang melakukan pertukaran informasi pada *layer* 2 pada *switch* untuk dapat saling bertukar informasi pada VLAN, VTP bertujuan unuk memudahkan administrator jaringan dalam konfigurasi VLAN pada perangkat *switch* yang jumlahnya banyak dengan cara membagikan konfigurasi VLAN dari VTP server kepada VTP *client*. VTP merupakan hak milik dari Cisco yang berfungsi untuk *switch-switch* dapat saling terhubung dan bertukar informasi konfigurasi. Cara kerja VTP sendiri menetapkan perangkat yang menjadi server dan sebagai *client*, di mana *client* dapat menerima konfigurasi-konfigurasi pada pada *switch* server secara otomatis dengan memasukan domain yang sama[15].

Dalam penerapan protokol VTP dalam sebuah VLAN perlu diketahui adanya istilah-istilah yang ada dalam tahap konfigurasinya yang meliputi:

1. VTP Mode

   VTP mode merupakan beberapa pilihan mode yang tersedia dan bisa diaktifkan dalam sebuah perangkat *switch* yang akan menggunakan protokol VTP. Terdapat 3 mode pada konfigurasi VTP yang seperti pada gambar 2.5.



Gambar 2.5 mode-mode pada VTP[16]

Diantara beberapa mode yang tersedia pada VTP mode adalah:

a. VTP Mode Server

Mode server dalam sebuah protokol VTP diumpamakan seperti administrator di mana dalam mode server ini *switch* dapat mengubah, menambah, menghapus serta menyebarkan VLAN-VLAN kepada *switch* dengan mode VTP *client*.

b. VTP Mode *Transparent*

Pada mode *transparent* perangkat hanya berfungsi sebagai jembatan saja antara VTP server dengan VTP *client* tanpa terpengaruh adanya konfigurasi apapun. Dengan kata lain mode *transparent* tidak akan menyebarkan konfigurasinya kepada *switch-swtich* lain.

c. VTP Mode *Client*

Mode *client* pada protokol VTP hanya berfungsi sebagai penerima hasil konfigurasi pada VTP server, oleh karena itu mode *client* hanya sebagai

read only tidak dapat merubah atapun mengotak-atik konfigurasi yang tersedia.

2. VTP Domain

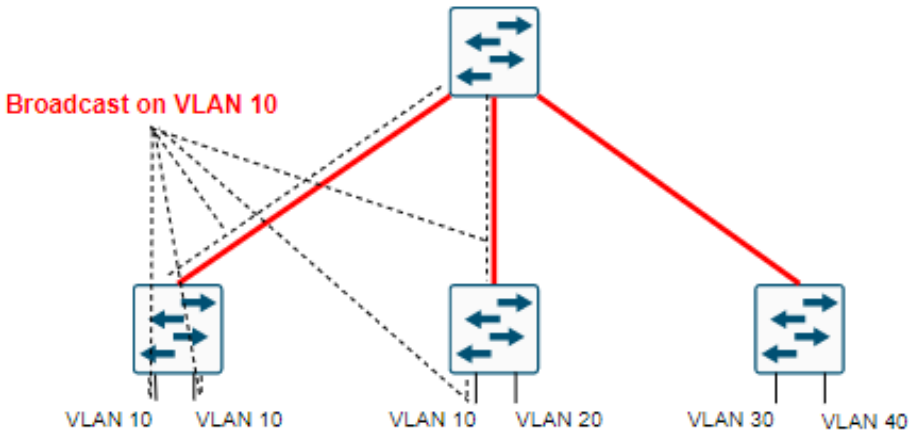
   VTP domain merupakan sebuah nama yang digunakan sebagai penanda, di mana nantinya akan membuat antara perangkat *switch* dengan domain yang sama dapat saling tergabung dan bertukar konfgurasi VLAN menggunakan VTP *advertisement.*

3. VTP *Advertisement*

   VTP *Advertisement* merupakan sebuah istilah untuk nama paket VTP yang berisikan informasi VLAN ID yang dibuat pada VTP server dan akan dikirimkan pada semua perangkat *switch* yang memiliki domain sama. VTP *advetisement* akan mengirimkan paket secara periodik setiap 5 menit oleh VTP server secara *multicast* dengan menggunakan MAC *address* perangkat.

4. VTP *pruning*

   VTP *prunning* merupakan sebuah vasilitas pada protokol VTP yang diaktifkan pada jalur *trunk* agar data tidak diteruskan dari vlan dengan nomor ID tertentu ke wilayah vlan yang lain.

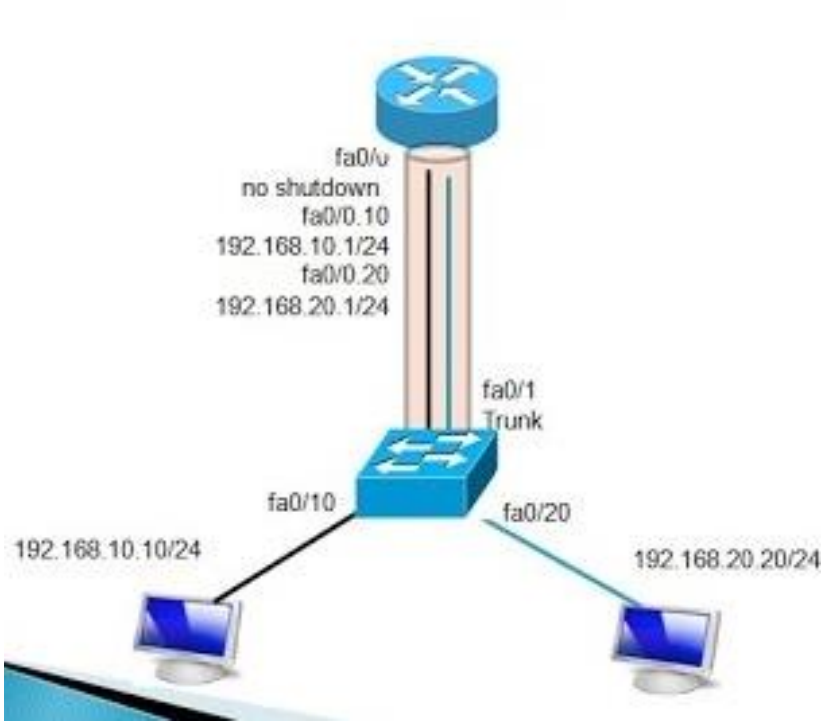


Gambar 2.6 Konsep VTP *prunning*[17]

VTP *prunning* digunakan untuk meningkatkan *bandwith* agar tidak membebani trafik jaringan terutama dalam penggunaan *bandwith* saluran. Contoh penerapan VTP *prunning* dapat dilihat pada gambar 2.6.

2.2.4 *Inter*-VLAN *Routing*

Secara *defaulth* VLAN sudah terbentuk akan tetapi masing-masing VLAN tidak dapat berkomunikasi satu sama lain. dalam kondisi ini VLAN memang sangat aman. setiap VLAN merupakan sebuah *broadcast* doamin yang unik. untuk membuat VLAN dapat berkomunikasi dengan VLAN yang lainya diperlukan adanya perutean antar VLAN (*Inter*-VLAN *Routing*)[18].



Gambar 2.7 *Inter*-VLAN dengan *Router On Stick*[19]

Inter-VLAN *Routing* memiliki dua konsep penerapan yang berbeda, *Multilayer switch* merupakan sebuah perangkat *switch* yang sering dikenal dan mampu melakukan perutean jaringan untuk *inter*-VLAN dan *router on stick* yang merupakan sebuah router yang mampu melakukan peroses *InterVLAN* yang dilakukan dengan menggunakan perangkat *router* untuk digunakan sebagai *gateway* masing-masing VLAN seperti pada gambar 2.7. Dari segi keanggotaanya VLAN dapat dibagi menjadi dua[20]:

1. VLAN Statis

VLAN static merupakan sebuah VLAN yang keanggotanya dibuat secara

manual dengan menetapkan *port* mana saja yang akan dimasukan ke dalam VLAN sehingga memiliki *broadcast* domain yang sama. Ketika perangkat terhubung ke *port*, secara otomatis mengasumsikan VLAN ke *port* yang ditetapkan. Dengan adanya VLAN statis ini dapat mengurangi adanya *broadcast* dan keamnan. Hal ini dikarena VLAN statis memiliki beban yang sangat kecil dan juga VLAN statis mampu menawarkan keamanan yang mempuni dibandingkan dengan *switch* tradisional.

2. VLAN Dinamis

VLAN dinamis merupakan sebuah VLAN yang dibuat dengan cara menetapkan host ke VLAN sehingga pada saat *host* terhubung ke *switch* menggunakan alamat MAC yang disimpan dalam database maka otomatis akan terhubung kedalam VLAN yang sudah ditentukan. VLAN dinamis memerlukan adanya server pusat yang disebut VLAN *Membership Policy Server* (VMPS). VMPS akan digunakan untuk mengatur konfigurasi *port* setiap *switch* pada VLAN. VMPS server berisi database yang berupa alamat MAC perangkat dengan VLAN yang dimilikinya. VLAN dinamis ini dapat memungkinkan *host* akan tetap terhubung kedalam VLAN yang sama walaupun dengan perangkat yang berbeda asalkan masih terlibat dalam jaringan VMPS.

2.2.5 Keamanan Jaringan

Keamanan komputer atau *Network security* merupakan suatu keamanan informasi yang diterapkan didalam sebuah sistem maupun pada infrasturktur jaringan. serta keamanan jaringan atau *Network Security* juga merupukan salah satu bagian dari keamanan komputer hanya saja lebih terfokus kepada keamanan infrastruktur jaringan ataupun keamanan jaringan merupakan bagian dari *cybersecurity*, sama seperti dengan *computer security* dan *information security* yang berpatok dengan prinsip CIA Triad, *network security* juga demikian. Tujuan dari keamanan jaringan komputer yaitu untuk mengantisipasi terjadinya resiko ancaman ataupun penyerangan baik berupa ancaman fisik maupun pencurian data yang dilakukan terhadap seseorang yang tidak berwenang[21].

Gambar 2.8 Aspek-aspek CIA *Triad*[22]

Pada gambar 2.8 merupakan aspek-aspek dalam CIA *triad.* eamanan pada sebuah sistem memiliki aspek-aspek yang terdiri dari 3 aspek penting yang disingkat menjadi *Confidentiality* (C), *Integrity* (I), *Availibility* (A) CIA[22]:

1. *Confidentiality*

Confidentiality atau kerahasiaan merupakan suatu properti bahwa suatu informasi tidak tersedia atau diungkap kepada individu, entitas atau dengan cara yang tidak sah. Informasi harus dijaga semaksimal mungkin untuk dijaga kerahasiaanya dari kebocoran yang disebabkan oleh individu ataupun entitas dari dalam maupun daru luar. *Confidentiality* memiliki dua hal penting pada penerapanya:

a. *Authentication*

   Ototentikasi merupakan sebuah sistem yang diterapkan untuk memungkinkan pengguna dapat masuk kedalam sebuah sistem. Ototentikasi ini dapat memuat berupa kata sandi dan teknik untuk identitas seperi biometrik, kriptografi dan yang lainya.

b. *Authorization*

   Otorisasi merupakan sebuah cara untnuk menentukan seseorang berhak untuk mengakses ataupun tidak kedalam sebuah sistem. Tanda pengenal dapat menjadi cara agar sistem dapat mengenali pengguna namun tidak semua pengguna semua pengguna dapat mengakses sebuah data ataupun menggunakan fitur tertentu pada sistem.

2. *Integrity*

   Integrity atau integritasi dalam hal ini merupakan hal yang berhubungan dengan akurasi kelengkapan data dan informasi. Integritasi ini harus dijaga dan tidak boleh seorangpun untuk memodifikasi ataupun melakukan kejahatan terhadap data dan informasi. Hal ini bertujuan untuk melindungi suatu data dari adanya seseorang yang tidak berwenang untuk melakukan modifikasi ataupun penghapusan data.

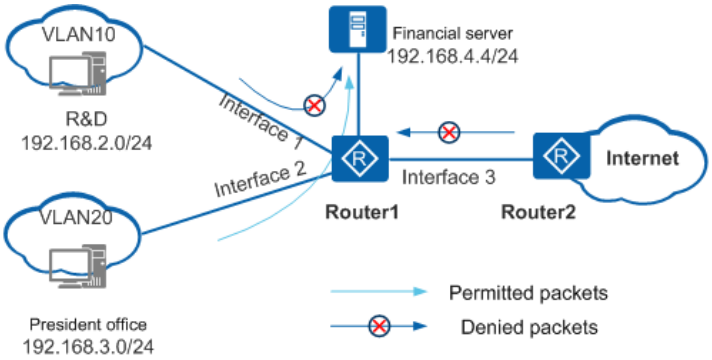
   Teknik yang digunakan bertujuan untuk menjaga integritas dari suatu data, hal ini dapat dilakukan dengan cara aturan untuk seseorang melakukan pengaksesan terhadap data tertentu yang dilakukan terhadap sebagian operasi sistem.

3. *Availability*

   Availibility atau ketersediaan sistem merupakan kemudahan akses serta penggunaan yang disesuaikan dengan permintaan seseorang yang berwenang. Pengguna/*user* yang memiliki hak kewenangan dapat mengakses informasi ataupun data kapanpun dan di manapun jika hal itu perlu dilakukan.

2.2.6 *Access Control List* (ACL)

Access Control List (ACL) merupakan sebuah aturan dalam jaringan yang digunakan sebagai pengontrol trafik data berdasarkan kriteria tertentu. Maksud dari kontrol adalah mengizinkan (*allow)* ataupun tidak mengizinkan (*deny*) suatu paket untuk diteruskan sampai ketujuan.

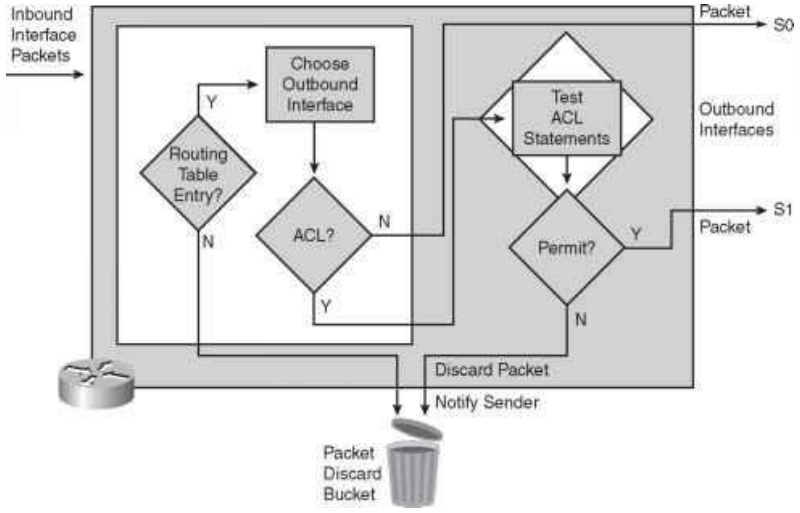


Gambar 2.9 Gambaran penggunaan ACL[23]

Perangkat yang memungkinkan untuk dikonfigurasi *Access Control List* yaitu berupa router ataupun *multilayerswitch*[23]. Gambar 2.9 merupakan penerapan dari *access control list.*

1. Cara Kerja ACL

Pada penerapanya ACL akan ditetapkan pada *interface* router ataupun *multilayer switch*. *Interface* itu sendiri terbagi menjadi 2 bagian berupa *IN* dan *OUT*[24]. Gambar 2.10 merupakan perbedaan cara kerja *inbound* dan *outbound* ACL.



Gambar 2.10 Diagram alir *Inbound* ACL dan *Outbound* ACL[25]

a. *Inbound* ACL

Ketika paket masuk pada sebuah *interface* router ataupun *multilayer switch*, lalu isi paket tersebut akan dilihat *header*-nya. *Header* pada sebuah paket dapat terbagi menjadi dua bagian berupa alamat IP pengirim dan alamat IP penerima ataupun bisa menggunakan sebuah aturan dengan penggunaan *port*.

ACL yang ditetapkan *interface* IN (*Inbound*) maka akan bekerja secara berurutan dan dilakukan dengan pencocokan sesuai dengan baris perintah yang ditentukan. Apabila ada sebuah baris yang cocok maka baris selanjutnya tidak akan dilakukan pencocokan lagi, selanjutnya paket akan dilihat apakah paket itu akan diteruskan ataupun ditolak jika paket ditolak maka isi paket tersebut akan dibuang dan apabila diterima (*permit*) maka paket akan diteruskan untuk melalui proses *routing*.

b. *Outbound* ACL

Proses kerja *outbound* ACL akan dimulai ketika paket diteruskan menggunakan proses *routing*, pada proses ini akan dilihat alamat IP yang digunakan pada penerima. Perangkat router ataupun *multilayer*

switch akan mencocokan informasi yang tersedia pada tabel *routing*, jika tidak ditemukanya tabel *routing* yang cocok maka paket tersebut akan dibuang dan jika paket tersebut cocok dengan alamat IP penerima maka paket akan diteruskan melalui *interface* yang dipilih. Selain itu pencocokan aturan ACL juga berlaku di mana paket akan dilihat alamat IP nya apakah aturan yang dibuat memperbolehkan untuk disampaikan ketujuan (*permit*) ataupun tidak diperbolehkan untuk sampai ketujuan (*deny*).

2. Tipe-tipe ACL

   Sebuah perusahaan perangkat jaringan cisco mengkategorikan ACL menjadi dua bagian yaitu tipe *standard* ACL dan *extended* ACL.

   a. *Standard* ACL

   Standard ACL melakukan pengecekan pada sebuah paket hanya sampai *layer* 3 (*network*). Tipe ACL ini akan melakukan *filtering* terhadang suatu host tertentu dan tidak dapat melakukan pemilihan protokol yang akan di *filter*. Penomoran yang ditentukan untuk standard ACL yaitu dari 1 hingga 99.

   b. *Extended* ACL

   Extended ACL melakukan pengecekan hingga pada *layer* 4 (*transport*) dengan dilakukan pengecekan hingga nomor *port* (*port number*) yang bertujuan untuk mengetahuin apa saja layanan yang akan dituju oleh data yang dikirimkan oleh komputer seperti www, ftp, sftp dan lainnya. Tipe ACL *Exended* memiliki penomoran dari 100 hingga 199.

2.2.7 *QUALITY OF SERVICE* (QOS)

Quality Of Service (QOS) merupakan sebuah metode pengukuran dalam meniai seberapa baik jaringan yang digunakan serta QoS merupakan suatu cara dalam mendefinisikan sifat dari suatu *service* jaringan. QoS digunakan untuk mengukur sekumpulan perangkat kinerja yang telah dispesifikan dan diasosiasikan dengan suatu servis yang ada[28].

QoS memiliki beberapa parameter untuk menentukan baik atau buruknya suatu servis yang diberikan, berikut merupakan parameter-parameter yang digunakan dalam pengukuran QoS:

1. *Throughput*

Throughput merupakan kecepatan (*rate*) transfer suatu data secara efektif, yang diukur dalam satuan bps (*bit* per *second*). *Throughput* adalah jumlah total kedatangan paket data yang sukses diamati dari sumber sampai tujuan selama jarak waktu tertentu dan dibagi oleh durasi jarak waktu tersebut[28]. Rumus *throughput* terdapat pada Persamaan 2.1.

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

2. *Packet Loss*

Packet Loss adalah suatu parameter dalam QoS yang menentukan suatu kondisi berapa banyak jumlah total paket yang hilang, *packet Loss* dapat terjadi karena *collision* dan *congestion* pada suatu jaringan[28]. Rumus *packet loss* terdapat pada Persamaan 2.2.

$$\boldsymbol{packet\ loss} = \frac{(paket\ data\ dikirim - paket\ data\ diterima)x100\%}{paket\ data\ dikirim} = \ \% \qquad (2.2)$$

3. *Delay* (*Latency*)

Delay (*latency*) merupakan waktu yang dibutuhkan data dalam menempuh suatu jarak dari asal (*source*) ke tujuan (*destination*). Nilai *delay* dapat dipengaruhi oleh jarak, media fisik, *congestion* dan juga waktu proses yang lama[28]. Rumus *delay* terdapat pada persamaan 2.3.

$$\boldsymbol{Delay} = \frac{total\ delay}{total\ paket\ diterima} = \ ms \qquad (2.3)$$

4. *Jitter*

Jitter dapat diakibatkan oleh varias-variasi dalam panjang antrian, dalam waktu pengolahan data, dan juga dalam waktu penghimpunan ulang paket-paket diakhir perjalanan *jitter*[28]. Rumus *Jitter* terdapat pada Persamaan 2.4

$$\textbf{\textit{Jitter}} = \frac{total\ variasi\ delay}{total\ paket\ diterima - 1} = \quad ms \tag{2.4}$$