# Perancangan *Firewall* dan *Spanning Tree Protocol* sebagai Sistem Keamanan Jaringan Komputer

**Aldi Adisty Putra[1)], Ispandi[2)], Baginda Oloan Lubis[*)3)]**

[1)2)] Fakultas Teknologi Informasi, Universitas Nusa Mandiri
[3)] Fakultas Teknik dan Informatika, Universitas Bina Sarana Informatika
[*)]Correspondence Author: baginda.bio@bsi.ac.id, Jakarta, Indonesia
**DOI:** https://doi.org/10.37012/jtik.v9i1.1340

## Abstrak

Dalam mengimplementasikan *firewall* di perusahaan, yang menjadi perhatian adalah perangkat yang digunakan, karena implementasi *firewall* pada setiap perangkat berbeda, misalnya *router* Mikrotik berbeda dengan implementasi *firewall* pada *router Cisco route*. *Firewall* ini digunakan untuk menyaring paket yang akan masuk ke jaringan perusahaan dan sebaliknya. Dengan demikian, jaringan perusahaan dapat menjamin keamanan informasi yang masuk atau keluar jaringan. Berdasarkan dari permasalahan yang ada, penelitian dimaksudkan untuk merancang dan menerapkan *filtering* data pada *firewall* dengan menggunakan *Access Control List.* Tujuan dari penelitian ini merancang *firewall* pada *router cisco* sebagai mekanisme keamanan jalur informasi yang masuk dan keluar dari jaringan komputer pada suatu perusahaan. Konfigurasi *access control list* diterapkan sebagai *firewall* untuk menyaring setiap paket data yang masuk dan keluar dari jaringan komputer perusahaan. Manajemen setiap *host* yang ada di dalam jaringan komputer dapat digunakan untuk melakukan koneksi keluar dan masuk pada jaringan komputer sebagai penghematan *bandwidth*. Hasil dari penelitian ini dengan mengaktifkan *firewall* menggunakan *feature Access Control List* (ACL) dapat digunakan untuk memblok situs yang dianggap tidak ada relevan dengan kebutuhan kerja dari perusahaan.

**Kata Kunci:** *Firewall, Filtering, Spanning Tree Protocol,* Keamanan Jaringan Komputer

## *Abstract*

*In implementing a firewall in a company, what matters is the device used, because the firewall implementation on each device is different, for example a Mikrotik router is different from the firewall implementation on a Cisco route router. This firewall is used to filter packets that will enter the corporate network and vice versa. Thus, the corporate network can guarantee the security of information entering or leaving the network. Based on the existing problems, the research is intended to design and implement data filtering on firewalls using an Access Control List. The purpose of this study is to design a firewall on a Cisco router as a security mechanism for information flow into and out of a computer network in a company. The access control list configuration is implemented as a firewall to filter every data packet that enters and leaves the company's computer network. Management of each host in a computer network can be used to make outgoing and incoming connections on a computer network as bandwidth savings. The results of this study by activating the firewall using the Access Control List (ACL) feature can be used to block sites that are deemed irrelevant to the work needs of the company.*

***Keywords:*** *Firewall, Filtering, Spanning Tree Protocol, Computer Network Security*

## PENDAHULUAN

Kebutuhan akan informasi yang *realtime* sangatlah penting. Untuk mendapatkannya secara cepat bahkan secara langsung harus didukung oleh koneksi jaringan internet yang cepat dan stabil. Selain itu juga harus dapat melindungi koneksi jaringan dari segala macam

ancaman yang dapat mengganggu koneksitas dari koneksi tersebut. Gangguan koneksi pada jaringan salah satunya adalah terjadinya *network looping* pada perangkat *intermediary* seperti *switch*. Pengiriman paket data yang berulang dengan paket yang sama melewati *switch* yang sama dengan *port* yang berbeda dan diteruskan secara *broadcast* atau dengan kata lain dapat mengurangi *network looping*. (Alifyaa et al., 2017)

Dengan terjadinya *network looping* maka sistem jaringan yang ada akan menjadi sibuk karena banyaknya paket data yang berjalan pada lalu lintas jaringan komputer tersebut. Belum lagi ditambah beban jika berbicara sistem proses bisnis pada perusahaan yang memungkinkan sistem kerja jaringan akan menjadi lebih sibuk lagi. Karena paket data pada lalu lintas jaringan yang menghubungkan satu perangkat jaringan komputer ke perangkat jaringan komputer lainnya harus dioptimalkan. Sehingga dampak yang terjadi dan yang dirasakan oleh pengguna dengan sistem jaringan komputer tersebut dapat diatasi. Dampak yang akan terjadi adalah jaringan menjadi lambat, atau bisa juga paket data yang dikirim akan terjadi tabrakan sehingga paket data tersebut tidak dapat diterima oleh perangkat jaringan tujuan atau paket data yang diterima mengalami kerusakan.

Menurut Plt. Kepala Pusopskamsinas BSSN, Adi Nugroho yang dirilis oleh koran tempo tanggal 1 Maret 2021 “Pada 2020, BSSN mendeteksi 495.337.202 serangan siber terjadi di Indonesia dengan serangan terbanyak berupa *malware trojan* yang dapat merusak suatu sistem ataupun mencuri data. Dalam penerapan *firewall* di perusahaan, yang menjadi perhatian adalah perangkat yang digunakan, dikarenakan implementasi *firewall* pada setiap perangkat berbeda-beda, contohnya adalah pada *router mikrotik* berbeda dengan penerapan *firewall* pada *router cisco*. Pemanfaatan *firewall* ini digunakan untuk menyaring paket-paket data yang akan masuk ke dalam jaringan menuju keluar jaringan dan sebaliknya. Sehingga pada jaringan dapat memastikan informasi yang masuk ataupun keluar jaringan berjalan dengan aman.

Untuk dapat menjalankan tujuannya, sebuah *firewall* mempunyai empat teknik dalam mengontrol akses dan menegakkan kebijakan keamanan yang diterapkannya. Secara original, *firewall* terfokus pada keutamaan dalam mengontrol pelayanan, yaitu :

1. *Service Control,* Menentukan jenis layanan internet yang dapat diakses, *inbound* atau *outbound*. *Firewall* dapat menyaring lalu lintas atas dasar alamat IP, protokol, atau nomor *port*; dapat menyediakan *software proxy* yang menerima dan menafsirkan setiap permintaan layanan sebelum dilewati atau mungkin *host server* perangkat lunak itu sendiri, seperti *web* atau layanan *mail*.

2. *Direction Control*, Menentukan arah layanan tertentu di mana permintaan dapat dimulai dan dibiarkan mengalir melalui *firewall.*
3. *User Control*, Kontrol akses terhadap pengguna dengan layanan sesuai mencoba mengaksesnya. Fitur ini biasanya diterapkan untuk pengguna di dalam *firewall* perimeter *(user local)*. Hal ini juga dapat diterapkan untuk lalu lintas masuk dari pengguna eksternal; yang terakhir membutuhkan beberapa bentuk teknologi otentikasi, seperti disediakan dalam *Ipsec.*
4. *Behavior Control*, Mengontrol bagaimana layanan tertentu yang digunakan. Sebagai contoh, *firewall* dapat menyaring *e-mail* untuk menghilangkan *spam*, atau memungkinkan akses eksternal untuk hanya sebagian dari informasi pada *server web* lokal.

Menurut (Setyawan, 2017) bahwa : "Dengan empat teknik tersebut diatas implementasi *firewall* dapat menjalankan penyaringan paket, maka diberlakukan seperangkat aturan untuk setiap paket IP yang masuk dan yang keluar dan kemudian bisa dibiarkan untuk dilewati atau membuang paket tersebut. *Firewall* biasanya dikonfigurasi untuk penyaringan paket di kedua arah (dari dan ke internal jaringan). Aturan penyaringan didasarkan pada informasi yang terkandung dalam sebuah paket jaringan.

Dalam penelitian sebelumnya dijelaskan bahwa *Spanning Tree Protocol* (STP) menyediakan jalur *backup* pada topologi yang berpotensi memiliki jalur *redudant.* Penerapan jalur *backup* terlihat bahwa STP dapat mencegah terjadinya *loop* dan *broadcast storm* yang mengakibatkan performa jaringan menurun. (Renwarin & Radiyah, 2021).

Kemudian dipenelitian yang lain menjelaskan bahwa dengan VLAN dapat dibuat segment yang berbeda, sedangkan dengan LAN fisik hanya bias membuat 1 segment saja, dengan begitu lalu lintas data akan tinggi. Dari permasalahan di atas diimplementasikan *Virtual Local Area Network* dengan *Switch Port* pada PT. Maxindo Mitra Solusi, sebagai solusi pemisah *network* antar divisi dengan menggunkanan satu perangkat fisik. (Ramadhan & Wijonarko, 2020)

Penelitian berikutnya menjelaskan sistem keamanan jaringan menjadi faktor yang sangat penting untuk dipertimbangkan bagi seorang administrator jaringan, dan berbagai upaya dilakukan dalam mengamankan jaringan dari ancaman dan serangan baik oleh *hacker* maupun penyebaran virus. *Access Control List* (ACL) merupakan salah satu alternatif upaya untuk mengamankan jaringan komputer. (Simamora et al., 2011)

Maksud dari penelitian ini untuk mengatasi permasalahan tabrakan paket data, *broadcast* domain, sebagai sistem cadangan terhadap jalur fisik yang terjadi pada perangkat

*intermediary switch* dengan menggunakan metode *Spanning Tree Protocol* (STP) pada perangkat *intermediary switch*. Kemudian merancang *firewall* pada *router cisco* sebagai keamanan jalur informasi yang masuk dan keluar dari jaringan komputer. Konfigurasi *Access Control List* sebagai implementasi *firewall* untuk menyaring setiap paket data yang masuk dan keluar dari jaringan computer, dan memanage setiap host yang ada di dalam jaringan komputer agar melakukan koneksi keluar dan masuk pada jaringan komputer sebagai penghematan *bandwidth*. Berdasarkan dari permasalahan yang telah dijabarkan, disini diteliti penerapan *filtering* data pada *Firewall* dengan menggunakan *Access Control List*.

## METODE

Penelitian ini dilakukan melalui beberapa aktifitas, yaitu analisa kebutuhan, desain, testing dan implementasi. (Hidayat et al., 2020). Analisis penelitian dilaksanakan dengan mengidentifikasi kebutuhan yang diperlukan untuk merancang *Spanning Tree Protocol* dan *Firewall* tersebut. Tahapannya sebagai berikut:

1. Analisa Kebutuhan

   Peralatan yang dibutuhkan untuk merancang dalam membangun *Firewall*, *Spanning Tree Protocol (STP)* diantaranya : Simulator *Software* Paket *Tracer* sebagai gambaran sistem jaringan yang akan dirancang.

2. Desain

   Sistem implementasi jaringan yang sudah menggunakan VLAN (*Virtual Local Area Network*) sebagai sistem cadangan koneksi fisik yang menghubungkan perangkat antar *intermediary* menggunakan *Spanning Tree Protocol*. Perancangan *Firewall* dengan *Access Control List* dengan membentuk topologi *tree* (pohon) dengan menggunakan metode *Wildcard Mask*, hal ini perlu dilakukan sebagai *filtering host* yang diberikan izin koneksi keluar atau masuk ke dalam jaringan komputer.

3. *Testing*

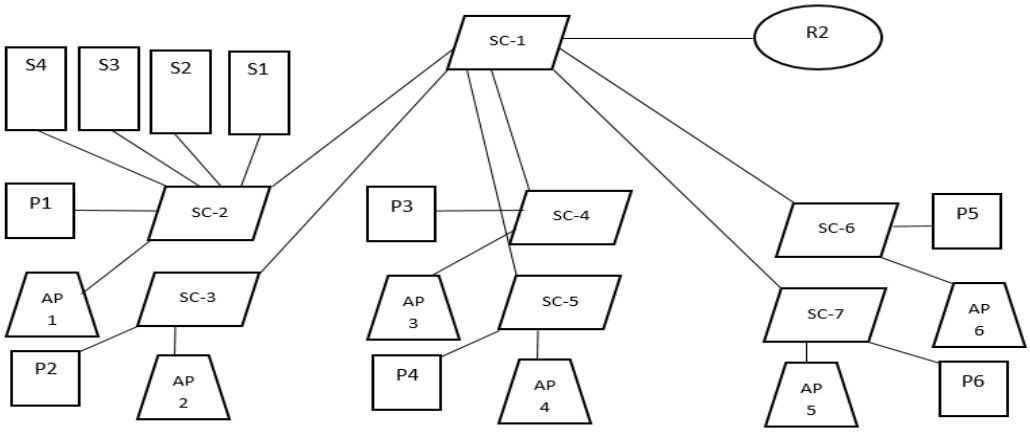
   Pada tahap ini rancangan jaringan menggunakan metode STP dan *Firewall* dengan menggunakan *Access Control List* dilakukan dengan cara peragaan secara virtual menggunakan simulator *Packet Tracer*.

4. Implementasi

   Implementasi dilakukan dengan cara mensimulasikan mengunakan aplikasi Packet Tracer dengan menyesuaikan skema jaringan komputer.

Dalam analisis topologi jaringan, digambar skema jaringan berdasarkan blok jaringan agar mudah dipahami, blok jaringan antara lain adalah :

1. S adalah *Server*
2. R adalah *Router*
3. SC adalah *Switch Catalist / Switch Multi layer*
4. P adalah PC
5. AP adalah *Access Point*

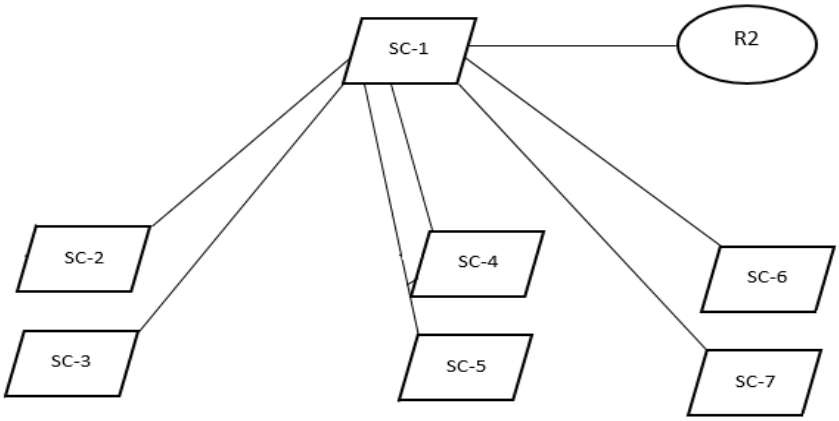



Sumber : Objek Penelitian (2022)

**Gambar 1.** Topologi Jaringan Berjalan

Dalam menganalisis topologi jaringan yang digunakan, peneliti membagi beberapa kelompok perangkat berdasarkan gambar topologi jaringan diatas, pembahasannya antara lain adalah :

1. Kelompok perangkat jaringan komputer pertama teridir dari : *Router* (R2), *Switch Multilayer* (SC1), *Switch Catalist 2* (SC2), *Switch Catalist 3* (SC3), *Switch Catalist 4* (SC4), *Switch Catalist 5* (SC5), *Switch Catalist 6* (SC6), *Switch Catalist 7* (SC7). Maka gambar blok jaringan seperti dibawah ini :

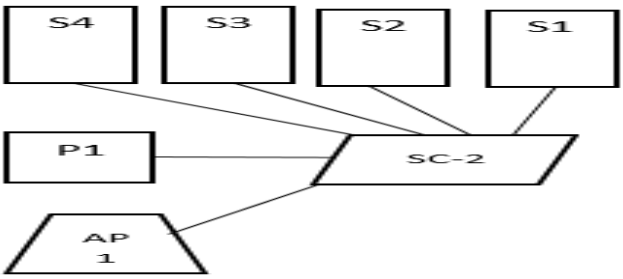



Sumber : Objek Penelitian (2022)

**Gambar 2.** Kelompok Blok Jaringan Komputer Pertama

Berdasarkan kelompok perangkat jaringan komputer pertama peneliti menganalisis topologi yang digunakan adalah jenis star, dikarenakan *Switch Catalist 1* (SC1) sebagai pusat koneksi dan menyerupai bentuk bintang *(star)*.

2. Kelompok perangkat jaringan komputer ketiga terdiri dari : *Switch Catalist 2* (SC2), *Server Aplikasi 1* (S1), *Server Aplikasi 2* (S2), *Server Aplikasi 3* (S3), *Server Aplikasi 4* (S4), PC 1 (P1) dan *Access Point 1* (AP1). Maka gambar blok jaringan seperti dibawah ini :

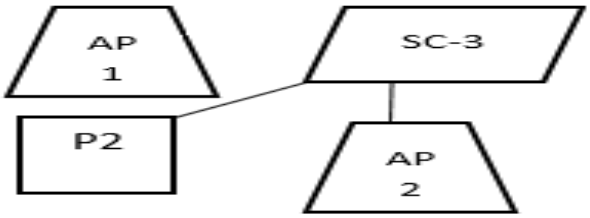



Sumber : Objek Penelitian (2022)

**Gambar 3.** Kelompok Blok Jaringan Komputer Kedua

Berdasarkan kelompok perangkat jaringan komputer ketiga peneliti menganalisis topologi yang digunakan adalah jenis *star*, dikarenakan *Switch Catalist 2* (SC2) sebagai pusat koneksi dan menyerupai bentuk bintang *(star)*.

3. Kelompok perangkat jaringan komputer ketiga teridiri dari : *Switch Catalist 3* (SC3), PC 2 (P2) dan *Access Point 2* (AP2). Maka gambar blok jaringan seperti dibawah ini :

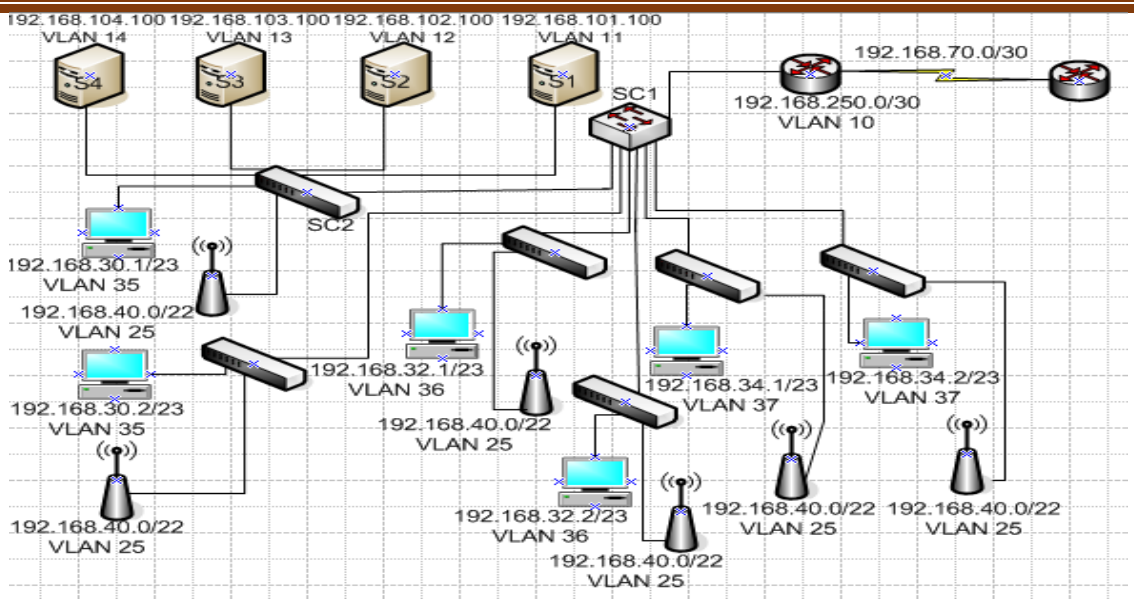



Sumber : Objek Penelitian (2022)

**Gambar 4.** Kelompok Blok Jaringan Komputer Ketiga

4. Kelompok perangkat jaringan komputer keempat dan seterusnya hampir sama dengan Kelompok jaringan Ketiga. Maka peneliti langsung menganalisis pada tiap kelompok jaringan komputer keempat dan seterusnya sampai kelompok jaringan kedelapan penulis menganalisis topologi yang digunakan adalah topologi star.

Berikut arsitektur jaringan yang menggambarkan secara umum perangkat-perangkat jaringan komputer yang digunakan:




Sumber : Objek Penelitian (2022)

**Gambar 5.** Skema Jaringan Berjalan

Peneliti mencoba menyimpulkan analisis semua segmen IP *Address* yang digunakan pada jaringan komputer berjalan sebagai berikut :

**Tabel 1.** Analisis Keseluruhan IP *Address*

| No | IP Address | Perangkat | Keterangan |
|---|---|---|---|
| 1. | 192.168.40.0/ 22 | Net Id ke 11 | 192.168.40.0 255.255.252.0 |
| | | Banyak Host Id | 192.168.40.1 s/d 192.168.43.254 |
| | | Almt Broadcast | 192.168.43.255 |
| 2. | 192.168.30.0/ 23 | Net Id ke 16 | 192.168.30.0 255.255.254.0 |
| | | Banyak Host Id | 192.168.30.1 s/d 192.168.31.254 |
| | | Almt Broadcast | 192.168.31.255 |
| 3. | 192.168.32.0/ 23 | Net Id ke 17 | 192.168.32.0 255.255.254.0 |
| | | Banyak Host Id | 192.168.32.1 s/d 192.168.33.254 |
| | | Almt Broadcast | 192.168.33.255 |
| 4. | 192.168.34.0/ 23 | Net Id ke 18 | 192.168.34.0 255.255.254.0 |
| | | Banyak Host Id | 192.168.34.1 s/d 192.168.35.254 |
| | | Almt Broadcast | 192.168.35.255 |
| 5. | 192.168.101.0/24 | Net Id ke 102 | 192.168.101.0 255.255.255.0 |
| | | Banyak Host Id | 192.168.101.1 s/d 192.168.101.254 |
| | | Almt Broadcast | 192.168.101.255 |
| 6. | 192.168.102.0/24 | Net Id ke 103 | 192.168.102.0 255.255.255.0 |
| | | Banyak Host Id | 192.168.102.1 s/d 192.168.102.254 |
| | | Almt Broadcast | 192.168.102.255 |
| 7. | 192.168.103.0/24 | Net Id ke 104 | 192.168.103.0 255.255.255.0 |
| | | Banyak Host Id | 192.168.103.1 s/d 192.168.103.254 |
| | | Almt Broadcast | 192.168.103.255 |
| 8. | 192.168.249.8/29 | Net Id ke 2 | 192.168.249.8 255.255.255.248 |
| | | Banyak Host Id | 192.168.249.9 s/d 192.168.249.14 |
| | | Almt Broadcast | 192.168.249.15 |

Sumber : Obejk Penelitian (2022)

Pada jaringan sistem berjalan menggunakan sistem keamanan jaringan di mulai dari:

1. Sudah terdapat sistem metode VLAN (*Virtual Local Area Network*) yang membagi beberapa logic jalur koneksi berdasarkan VLAN tersebut. VLAN ini digunakan untuk

mengamankan data atau informasi dari satu bagian atau divisi terhadap bagian atau divisi lain agar tidak dapat discanning. Selain itu juga jika salah bagian terkena virus atau *worm* atau *trojan* atau lainnya, maka dengan adanya VLAN bagian atau divisi ini akan secara otomatis mengisolasi hanya bagian atau divisi tersebut saja yang terjangkit dan tidak akan menyebar ke bagian atau divisi lainnya.

2. Sudah adanya manajemen IP Address ini terlihat berdasarkan IP Address yang digunakan beberapa sudah ada yang mengalami *subnetting.* Ini difungsikan agar IP *Address* yang digunakan secara terbatas dan tidak luas atau tidak banyak sehingga tidak dapat *user* mengganti-ganti IP *Address* seamaunya sendiri.
3. Untuk keamanan jaringan koneksi internet hirarki perangkat setelah modem langsung terhubung ke router, ini merupakan sebuah metode pencegahan agar koneksi internet dapat lebih dimanajemen pada *router.* Karena perangkat *router* yang memiliki *feature* untuk melakukan manajemen jaringan secara lebih baik dibandingkan dengan modem.
4. Dari segi keamanan jaringan *Hotspot* atau WiFI menggunakan pemfilteran atau penyaringan MAC *Address.* Hanya MAC *Address* yang sudah terdaftar pada Divisi IT dapat menggunakan jaringan *Hotspot* atau WiFI ini.

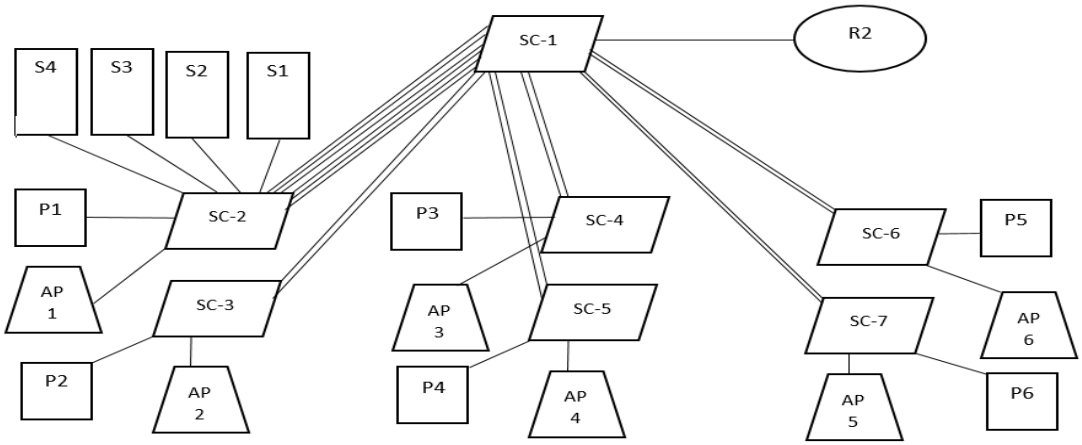
Pada jaringan sistem berjalan yang terdiri dari 3 lantai, yaitu Lantai 25 sampai dengan Lantai 27 yang menjadi pokok bahasan penelitian terdapat permasalahan pokok antara lain :

1. Koneksi jalur VLAN pada *Switch Catalist 2* (SC2) ke *Switch Multilaye*r (SC1) menggunakan satu buah koneksi kabel, koneksi tersebut sebagai VTP Trunk. Ini berisiko sekali jika satu kabel tersebut mengalami gangguan koneksi atau terputus yang bisa saja diakibatkan digigit hewan pengerat atau terkena bencana alam seperti tersambar petir ini akan mengakibatkan 4 server, sebagian *client* lantai 25 dan salah satu akses *point* akan tidak koneksi ke jaringan,
2. Pembatasan hak akses koneksi internet yang terhubung ke sistem pada setiap *client* dengan berbagai divisi atau bagian bebas melakukan koneksi. Sebaiknya dibatasi untuk pengaksesan pada setiap divisi atau bagian yang hanya berkepentingan saja sesuai dengan tanggung jawab dan kebutuhan kerja berdasarkan bagian atau divisi tersebut.
3. Koneksi jalur yang tersebar pada setiap lantai yang memiliki VLAN yang berbeda mempunyai 1 buah koneksi jalur fisik, jika 1 jalur ini terputus maka dalam 1 lantai tersebut akan terputus konseksinya. Maka disini memerlukan jalur fisik cadangan yang dapat membackup jalur utama VLAN pada setiap lantainya.

# HASIL DAN PEMBAHASAN

Untuk dapat memfilter data yang masuk maupun yang keluar dari jaringan memerlukan sebuah metode *Access Control List* atau yang disebut juga dengan ACL. ACL ini merupakan sebuah *feature* yang terdapat dalam *Router Cisco*, dan dalam penelitian ini dicoba pengimplementasian ACL dengan jenis *Extended* dengan nomor id antara 100 sampai dengan 199. Karena dengan ACL berjenis *extended firewall* dapat memfilter spesifik dari data yang ingin difilternya secara lebih detail.

Topologi jaringan yang diusulkan tidak merubah topologi yang saat ini ada didalam jaringan. Dalam penelitian dianalisis jika terjadi gangguan koneksi dengan terputusnya media transmisi kabel yang menghubungkan semua SC *(Switch Catalist)* dengan SC 1 akan mengakibatkan koneksi untuk semua perangkat jaringan yang ada tidak terkoneksi. Maka diperlukan jalur koneksi cadangan atau membantu dari koneksi utama pada semua SC, agar jika salah satu jalur (kabel yang menghubungkan antar SC) terputus mempunyai jalur kabel cadangan yang menghubungkan antar SC. Dan keuntungan lainya adalah yang awalnya koneksi jalur kabel sebagai penghubung antar SC hanya 1 koneksi kabel saat ini akan dilakukan pembuatan jalur koneksi kabel cadangan maka akan terjadi penambahan *bandwidth* pada jalur tersebut apalagi konsep ini diterapkan pada jaringan VLAN, inilah salah satu metode dalam jaringan yang disebut dengan *Spanning Tree Protocol* (STP).

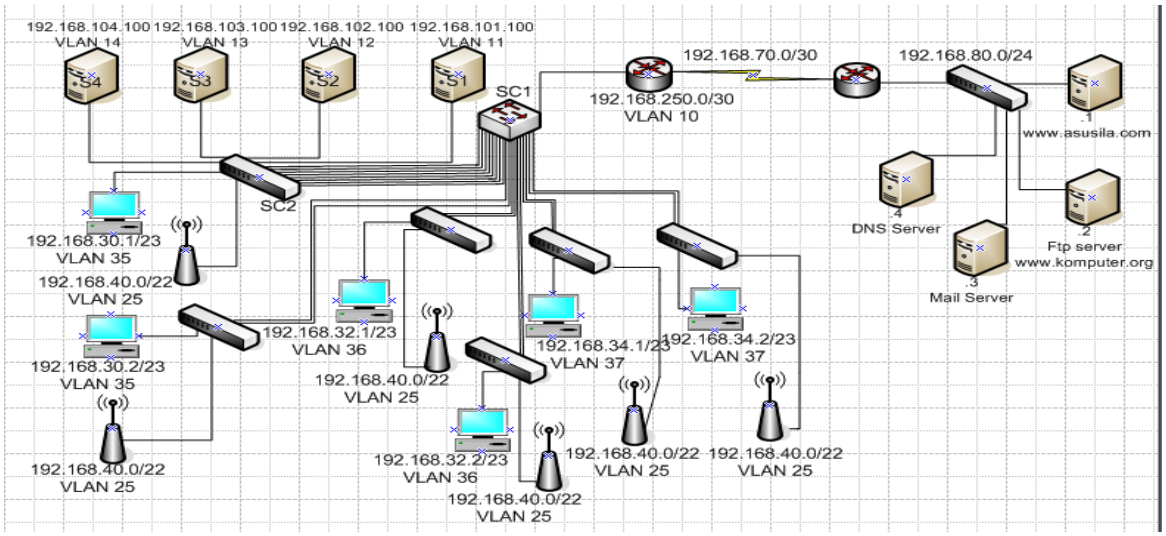



Sumber : Hasil Penelitian (2022)

**Gambar 6.** Topologi Jaringan Usulan

Pada bentuk skema jaringan yang dirancang, perangkat *Switch Catalist* (SC 2) yang menghubungkan server-server aplikasi dengan setiap server memiliki jalur virtual yang berbeda yaitu VLAN 11 untuk server 1, VLAN 12 untuk server 2, VLAN 13 untuk server 3 dan VLAN 14 untuk server 4. Peneliti mencoba rancangan dengan skema jaringan menambahkan 4 buah koneksi kabel sehingga kabel yang menghubungkan SC2 dengan SC1 sebanyak 5 koneksi kabel. 5 (lima) koneksi kabel tersebut penggunaannya adalah, 1 koneksi

sebagai jalur koneksi VLAN Client1, 1 koneksi sebagai jalur koneksi VLAN Server 1, 1 koneksi sebagai jalur koneksi VLAN Server 2, 1 koneksi sebagai jalur koneksi VLAN Server 3, 1 koneksi sebagai jalur koneksi VLAN Server 4. Dengan metode VTP Access (*Virtual Trunking Protocol*). Selanjutnya perangkat yang dikembangkan kemampuannya adalah Router 1, pada perangkat router terdapat feature *Access Control List* (ACL). Dengan metode ACL extended dicoba membangun sebuah firewall yang berguna menyaring paket data yang berada pada server yang terhubung dengan Router yang berada diseberang Router 1 (R1).




Sumber : Hasil Penelitian (2022)

**Gambar 7.** Topologi Jaringan Usulan

Untuk sistem keamanan jaringan dilakukan penambahan berupa pengaktifan *firewall* dengan menggunakan feature *Access Conrol List* (ACL). Dengan memfilter paket data yang dapat masuk maupun yang keluar dari jaringan. Selain memfilter peneliti juga menambahkan pemblokan akses internet pada sebuah situs yang dianggap merugikan (situs porno), selain itu juga peneliti membatasi akses client-client yang dapat melakukan koneksi internet secara akses full atau tidak.

Pada jaringan usulan ini peneliti membagi beberapa pokok materi yang menjadi usulan pada penelitian ini, antara lain adalah :

A. Merubah koneksi *Virtual Trunking Protocol* (VTP) mode Trunk dengan VTP mode Access.

   Alasan penulis jika adanya media transmisi kabel yang menghubungkan antara SC 1 (Switch Catalist) dengan SC 2 sebagai VTP metode Trunk yang berada di lantai 26 terputus (dikarenakan dimakan hewan pengerat, atau karena alam tersambar petir dan alasan lain-lainnya) tidak akan mengganggu koneksi VLAN lainnya (VLAN 35, VLAN 25, VLAN 11, VLAN 12, VLAN 13, dan VLAN 14).

Berikut ini design konfigurasi yang diusulkan:

**Tabel 2.** Design Usulan *Spanning Tree Protocol* (STP)

| Perangkat | Port | | Keterangan |
|---|---|---|---|
| SC2 –SC1 | **SC2** | **SC1** | Koneksi VTP Metode Trunk dan STP untuk semua VLAN |
| | Fa 0/10 | Fa 0/1 | |
| | Fa 0/11 | Fa 0/2 | |
| | Fa 0/12 | Fa 0/3 | |
| SC3 –SC1 | **SC3** | **SC1** | Koneksi VTP Metode Trunk dan STP untuk semua VLAN |
| | Fa 0/20 | Fa 0/4 | |
| | Fa 0/21 | Fa 0/5 | |
| SC4 –SC1 | **SC4** | **SC1** | Koneksi VTP Metode Trunk dan STP untuk semua VLAN |
| | Fa 0/20 | Fa 0/6 | |
| | Fa 0/21 | Fa 0/7 | |
| SC5 –SC1 | **SC5** | **SC1** | Koneksi VTP Metode Trunk dan STP untuk semua VLAN |
| | Fa 0/20 | Fa 0/8 | |
| | Fa 0/21 | Fa 0/9 | |
| SC6 –SC1 | **SC6** | **SC1** | Koneksi VTP Metode Trunk dan STP untuk semua VLAN |
| | Fa 0/20 | Fa 0/10 | |
| | Fa 0/21 | Fa 0/12 | |
| SC7 –SC1 | **SC7** | **SC1** | Koneksi VTP Metode Trunk dan STP untuk semua VLAN |
| | Fa 0/20 | Fa 0/13 | |
| | Fa 0/21 | Fa 0/14 | |

Sumber : Hasil Penelitian (2022)

B. Pembatasan akses salah satu kelompok Client pada koneksi internet

Didalam jaringan usulan ini peneliti menganalisis ada beberapa bagian atau divisi dapat mengakses sebuah sistem yang semestinya divisi atau bagian tersebut sebaiknya tidak boleh melakukan koneksi. Contohnya bagian divisi Marketing tidak dapat mengakses sebuah server *File Transfer Protocol* (FTP) yang berada pada jalur internet. Peneliti menganggap ftp server ini disediakan untuk keperluan di lapangan. Data-data penting apa yang ada dilapangan seperti: reporting struktur tanah BTS, lokasi atau medan pemasangan BTS dan lain-lainnya. Divisi atau bagian Marketing berada pada Lantai 26 dan kebetulan segmen IP Addrees yang dimiliki client-client pada Lantai 26 adalah 192.168.32.0/22.

Dengan adanya VTP metode Trunk dengan koneksi jalur fisik berupa kabel jaringan lebih dari satu buah untuk menghubungkan antar switch catalist yang ada di dalam perusahaan, peneliti berpendapat lebih baik memanajemen jaringan yang ada karena jalur koneksi VLAN yang ada pada Lantai 25 mempunyai lebih dari 1 buah jalur kabel sehingga jika terjadi kendala salah satu jalur kabel *down* atau terputus maka jalur kabel lainnya akan menggantikan secara otomatis sehingga koneksi semua antar switch catalist tidak ada terputus dan tetap terhubung satu sama lainnya. Sehingga divisi IT secara manajemen jaringan ada sistem pem-backup-an dalam sistem koneksi antar *switch catalist*nya.

Satu hal lagi tentang manajemen jaringan adalah dengan membatasi akses berdasarkan kelompok client atau divisi atau bagian yang tidak berkepentingan untuk mengakses dalam sistem. Sehingga server yang melayani permintaan tidak terlalu sibuk, sehingga koneksi pada client ke server lebih dapat terisolasi yang menyebabkan koneksi akan menjadi lebih lancar. Dan setiap permintaan ke server, server akan cepat merespon permintaan tersebut.

Pada pengujian jaringan peneliti mencoba mengambil kesimpulan berdasarkan permasalahan yang diangkat, antara lain adalah :

1. Perubahan sistem koneksi VTP Trunk

   Sesuai dengan pengujian yang dilakukan, semua kelompok perangkat jaringan yang ada pada lantai 25 berdasarkan VLAN dapat koneksi ke semua perangkat yang ada didalam perusahaan ini. Keuntungan dari sistem koneksi VTP trunk dengan menggunakan satu jalur kabel dapat menghubungkan atau sebagai jembatan penghubung dari beberapa VLAN atau lebih dari 1 VLAN saja. Sehingga secara maintenance lebih simpel dan mudah.
2. Pembuatan jalur cadangan dengan menggunakan metode *Spanning Tree Protocol* (STP) pada semua *switch catalist*.

   Sesuai dengan pengujian yang peneliti lakukan semua kelompok perangkat jaringan yang ada pada lantai 25 berdasarkan sistem cadangan terhadap jalur fisik yang menghubungkan *Switch Catalis* 1 dengan *Switch Catalis* 2 jika terjadi salah satu jalur fisik terputus atau *down*, maka ada jalur fisik lain yang melakukan pem-backup-an agar koneksi semua client-client baik yang terhubung secara kabel dan wireless tidak akan terganggu untuk dapat melakukan koneksi ke 4 server yang ada pada perusahaan ini.
3. Melakukan penyaringan (filter) paket data terhadap FTP server pada client lantai 26 (bagian atau divisi Marketing)

## KESIMPULAN DAN REKOMENDASI

Berdasarkan pembahasan yang sudah dibuat, maka dapat disimpulkan sebagai berikut:

1. Dengan menggunakan VTP (*Virtual Trunking Protocol*), mode Trunk setiap VLAN yang berada pada Switch yang berbeda dapat terhubung, dan mode Trunk ini memberikan link koneksi satu jalur kabel untuk digunakan lebih dari satu VLAN berkomunikasi dengan VLAN yang sama pada Switch yang berbeda.

2. Metode *Spanning Tree Protocol* (STP) sebagai jalan alternatif pemecahan masalah jikalau dengan menggunakan jalur kabel yang menghubungkan antar *switch catalist* mengalami putus koneksi, maka ada jalur fisik atau kabel lain yang dapat digunakan sebagai pem-backup-an dari jalur koneksi yang terputus tersebut.
3. Dengan mengaktifkan firewall menggunakan *feature Access Control List* (ACL) dapat digunakan untuk memblok situs yang dianggap tidak ada relevansi dengan kebutuhan kerja dari perusahaan.
4. Dengan lebih mengoptimalkan ACL dapat membuat hak akses pada sebuah sistem yang terhubung pada internet lebih efisien. Jadi sistem hanya dapat diakses pada client-client yang membutuhkan sistem tersebut.

## REFERENSI

Alifyaa, T. R., Iswahyudi, C., & Rakhmawati, R. Y. (2017). Implementasi Spanning Tree Protocol (STP) Dalam Perancangan Virtual Lacal Area Network (VLAN). *Jurnal JARKOM*, *5*(2), 96–102.

Hidayat, A. S., Sobari, S., Lubis, B. O., & Akhirianto, P. M. (2020). Connetivity Jaringan Public Dengan Satu ISP Menghubungkan Kantor Cabang Dengan Menggunakan Metode Metro Ethernet. *Jurnal Teknologi Informatika Dan Komputer*, *6*(2), 63–73. https://doi.org/10.37012/jtik.v6i2.288

Ramadhan, R. R., & Wijonarko, B. (2020). Implementasi Virtual Local Area Network Dengan Switch Port Pada PT. Maxindo Mitra Solusi Jakarta. *Inti Nusa MAndiri*, *14*(2), 203–210. https://ejournal.nusamandiri.ac.id/index.php/inti/article/view/1225/613

Renwarin, M. V. J., & Radiyah, U. (2021). Implementasi Spanning Tree Protocol (STP) Pada Perancangan Virtual Local Area Network (VLAN) Pada PT. Regalindo Sakti Jakarta. *JI-Tech*, *17*(1), 6–11.

Setyawan, A. (2017). Address Menggunakan Metode Access List Control Pada Router Cisco. *Journal Teknik Komputer Amik BSI*, *III*(1), 60–73.

Simamora, S. N. M. P., Hendrarini, N., & Sitepu, L. E. (2011). Metode Access Control List sebagai Solusi Alternatif Seleksi Permintaan Layanan Data Pada Koneksi Internet. *Jurnal Teknologi Informasi Politeknik Telkom*, *1*(1), 15–19.