



## **Optimalisasi VLAN dengan menentukan Trunk Link dan Access Link untuk Minimalisir Connection Failure**

*Optimize VLAN By Determining Trunk Link And Access Link To Minimize Connection Failure*

**Felix Wuryo Handono<sup>1</sup>, Hanafi Eko Darono<sup>2</sup>,  
Nanang Nuryadi<sup>3</sup>, Ade Suryanto<sup>4</sup>, Amir<sup>5\*</sup>**

Program Studi Sistem Informasi<sup>1,2</sup>, Program Studi Informatika<sup>3</sup>,  
Program Studi Teknik Industri<sup>4</sup>, Program Studi Sistem Informasi  
Kampus Kota Bogor<sup>5</sup>  
Fakultas Teknik Dan Informatika  
Universitas Bina Saraana Informatika

[felix@bsi.ac.id](mailto:felix@bsi.ac.id), [hanafi.haf@bsi.ac.id](mailto:hanafi.haf@bsi.ac.id), [nanang.nyd@bsi.ac.id](mailto:nanang.nyd@bsi.ac.id),  
[ade.ayo@bsi.ac.id](mailto:ade.ayo@bsi.ac.id), [amir.amr@bsi.ac.id](mailto:amir.amr@bsi.ac.id)\*

**Received:** 2024-11-06. **Revised:** 2024-11-26. **Accepted:** 2024-11-29.

**Issue Period:** Vol.8 No.2 (2024), Pp. 252-263

**Abstrak:** Perangkat jaringan menyebar dapat terhubung ke sesama VLAN dengan ID yang sama, yang tidak dalam satu switch dan terhubung dengan switch lain. Dapat dihubungkan dengan metode Trunking. Metode trunking terdapat dua jenis yaitu Trunk Link dan Access Link. Koneksi Trunk link terdapat kendala, jika koneksi kabel atau port pada switch yang menghubungkan antar switch itu terjadi connection failure maka kabel atau port switch tersebut tidak dapat dilewati oleh beberapa VLAN. Kendala tersebut diperlukannya koneksi metode trunking Access Link yang merupakan jalur koneksi satu buah kabel atau satu buah port switch hanya digunakan untuk menghubungkan satu buah ID VLAN yang sama. Tetapi access link terdapat kendala juga jika diterapkan pada seluruh jaringan LAN kebutuhan tersedianya port pada switch, sehingga harus menyediakan switch yang banyak. Dalam meminimalisir terjadinya connection failure pada VLAN yang diambil adalah menentukan koneksi Trunk link dan Access link pada jaringan LAN sebagai optimalisasi kinerja VLAN tetap berjalan.

**Kata kunci:** access link, trunk link, vlan

**Abstract:** Diffuse network devices can connect to fellow VLANs with the same ID, which are not in one switch and are connected to other switches. Can be connected with the Trunking method. There are two types of trunking methods, namely Trunk Link and Access Link. The Trunk link connection has problems, if the cable or port connection on the switch that connects the switches experiences a connection failure then the cable or switch port cannot be passed by some VLANs. This obstacle requires a connection using the Access Link trunking method, which is a connection line of one cable or one switch port only used to connect the same VLAN ID. However, access links also have problems if they are applied to the entire LAN network, which requires the availability of ports on switches, so many switches must be provided. To minimize the occurrence of connection failure on the VLAN, what is



DOI: 10.52362/jisicom.v8i2.1663

Ciptaan disebarluaskan di bawah [Lisensi Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/).



*taken is to determine the Trunk link and Access link connections on the LAN network to optimize the performance of the VLAN while continuing to run.*

**Keywords:** *access link, trunk link, vlan*

## I. PENDAHULUAN

Beberapa perusahaan modern yang terdiri dari beberapa lantai dan ruangan, tentunya sudah mempunyai teknologi jaringan komputer agar dapat terhubung pada setiap lantai untuk mendukung kegiatan operasional. Namun seiring dengan meningkatnya kebutuhan serta user, permasalahanpun timbul yang berkaitan dengan keamanan dan belum adanya jalur redudansi antar switch [1]. Dalam hal keamanan, penggunaan LAN konvensional memiliki resiko pembajakan informasi atau paket di dalam jaringan LAN itu sendiri. Hal tersebut dikarenakan setiap paket yang masuk dari jaringan luar akan didistribusikan ke semua workstation yang ada, mengingat jaringan hanya memiliki satu broadcast domain. Hal tersebut tentu kurang menguntungkan [2].

Bahwa dengan perkembangan jaringan teknologi, terutama pada perangkat lunak computer (dalam bentuk system operasi dan aplikasi), memungkinkan adanya konfigurasi dari suatu jaringan computer secara virtualisasi. VLAN merupakan salah satu solusi yang diberikan untuk hal tersebut [3]. Didalam penerapan segi keamanan dengan VLAN sudah terpenuhi dengan adanya pengamanan VLAN digunakan untuk mengamankan data atau informasi dari satu bagian atau divisi terhadap bagian atau divisi lain agar tidak dapat discanning. VLAN ini digunakan untuk mengamankan data atau informasi dari satu bagian atau divisi terhadap bagian atau divisi lain agar tidak dapat discanning.[4] 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 terjangkau dan tidak akan menyebar ke bagian atau divisi lainnya [5].

Setiap host atau computer atau perangkat jaringan computer yang menyebar didalam jaringan LAN dapat terhubung ke sesame VLAN dengan ID yang sama, yang tidak berada dalam satu switch dan mungkin tersebar didalam jaringan LAN yang terhubung dengan switch lain dapat terhubung ke sesame VLAN diperlukan sebuah metode yang disebut dengan *Trunking*. Jaringan LAN yang menghubungkan beberapa perangkat switch menggunakan konsep jalur *trunking* dalam mempertukarkan data antar perangkat switch [6]. 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 [7]. Metode trunking terdapat dua jenis yaitu *Trunk Link* dan *Access Link*. Kebutuhan akan adanya *Trunking VLAN* dengan metode *Trunk Link* membutuhkan satu koneksi kabel atau jalur fisik kabel atau satu buah port dalam satu switch pada setiap switch. Dikarenakan *trunk link* merupakan koneksi yang multi VLAN atau berkumpulnya ID VLAN-ID VLAN yang berbeda berjalan dalam satu buah jalur koneksi atau port yang menghubungkan antar switch.

Koneksi *Trunk link* ini juga terdapat kendala atau permasalahan, jika sebuah koneksi fisik kabel atau port pada switch yang menghubungkan antar switch itu terjadi *connection failure* atau *down* (mati) atau bisa juga port yang terdapat switch yang digunakan jalur *trunk link* tersebut mati (off) maka jalur fisik tersebut tidak dapat dilewati kembali oleh beberapa ID VLAN-ID VLAN yang ada. Jalur fisik kabel atau koneksi penghubung antar ID VLAN yang sama pada switch tidak cukup kuat juga jika *trunk link* ini digunakan untuk ID VLAN yang digunakan sebagai jalur perangkat server, artinya perangkat switch sebaiknya menggunakan VLAN ID yang berbeda satu sama lainnya agar pemeliharaan jalur koneksi VLAN lebih mudah diidentifikasi.

Jalur koneksi server juga yang berada didalam VLAN ID harus adanya pemisahan ID VLAN dengan ID VLAN host atau computer lainnya atau perangkat jaringan lainnya, agar koneksi dapat berjalan dengan baik saat komunikasi dengan server. Ini dikarenakan sebuah perangkat server merupakan jalur yang penting terhadap kegiatan bisnis didalam sebuah organisasi atau perusahaan. Oleh sebab koneksi kabel atau port pada switch itu harus terjaga dengan meminimalisir *connection failure* atau *down*, agar kegiatan bisnis sebuah organisasi atau perusahaan tetap terjaga.

Dari permasalahan tersebut diperlukannya adalah koneksi *trunking VLAN* dengan metode *Access Link* yang merupakan jalur koneksi satu buah kabel atau satu buah port pada switch hanya digunakan untuk





menghubungkan satu buah ID VLAN yang sama. Tetapi ada kendalanya jika penerapan *access link* ini diterapkan pada seluruh ID VLAN pada jaringan LAN. Kebutuhan akan tersedianya port pada switch amat sangat terbatas, sehingga sebuah organisasi atau perusahaan harus menyediakan switch yang banyak, karena banyaknya ID VLAN berbanding lurus dengan kebutuhan banyaknya port pada switch. Selain itu, agar dapat memberikan pandangan atau gambaran langkah terbaik dalam meminimalisir terjadinya *connection failure* pada VLAN yang diambil dalam memecahkan permasalahan tersebut. Menentukan koneksi Trunk link dan Access link pada perangkat jaringan LAN sebagai optimalisasi kinerja VLAN agar tetap berjalan sesuai dengan harapan dan tujuan kebijakan organisasi atau perusahaan. Dan untuk memberikan akses jalur VLAN yang terdapat pada alat-alat vital jaringan seperti server sebaiknya jangan digabungkan dengan perangkat lainnya. Sehingga jika terjadi permasalahan penanganan perbaikan dapat dilakukan dengan cepat, maka dibuat penelitian ini.

## II. METODE DAN MATERI

### 2.1. VLAN

Sekelompok host atau komputer dan server yang dikonfigurasi seolah-olah mereka berada di dalam LAN yang sama, meskipun mereka berada di seluruh router di LAN yang terpisah [8]. Terdapat 3 tipe VLAN, yaitu :

1. Port-Based VLAN

Komputer atau host yang terhubung ke port tertentu pada switch dimasukkan ke dalam VLAN tertentu.

2. Tagged-Based VLAN

ID VLAN yang digunakan berdasarkan protocol atau standar 802.1Q.

3. Protocol-Based VLAN

Koneksi ke port didasarkan pada protocol yang ada.

VLAN dibangun menggunakan berbagai perangkat, seperti: switch, router, PC dan sebagainya. Tentunya diperlukan hubungan atau link diantara perangkat-perangkat tersebut. Link seringkali disebut sebagai interface. Ada dua jenis link yang digunakan, yaitu:

1. Access Link

Merupakan tipe link yang umum dan dimiliki oleh hampir semua jenis switch VLAN. Accesslink lazimnya digunakan untuk menghubungkan komputer dengan switch. Access link tidak lain merupakan port switch yang sudah terkonfigurasi. Selama proses transfer data, switch akan membuang informasi tentang VLAN. Anggota suatu VLAN tidak bisa berkomunikasi dengan anggota VLAN yang lain, kecuali jika dihubungkan oleh router. Access link mendukung teknologi Ethernet biasa (10Mbps) hingga FastEthernet (100 MBps).

2. Trunk Link

Istilah Trunk diambil dari system telepon yang dapat mengangkat beberapa percakapan sekaligus (multiple conversation). Trunk Link digunakan untuk menghubungkan switch dengan switch yang lain, switch dengan router, atau switch dengan server. Jadi, port telah dikonfigurasi untuk dilalui berbagai VLAN (tidak hanya sebuah VLAN). TrunkLink hanya mendukung teknologi Fast (100Mbps) Ethernet atau Gigabit (1000Mbps) Ethernet. Sebab Trunk Link lazimnya dihubungkan dengan network backbone berkecepatan tinggi. Wajar jika kebutuhannya lebih tinggi dibandingkan Access Link [9].

Dalam penerapannya VLAN, Administrator jaringan harus memastikan port VLAN yang dibuat pada virtual machine sesuai dengan pada switch sebenarnya. Selain itu, setiap server virtual machine dipindahkan, maka administrator jaringan perlu melakukan konfigurasi ulan VLAN. Untuk mencocokkan fleksibilitas virtualisasi server, pengelola jaringan harus mampu untuk secara dinamis menambahkan, drop dan mengubah jaringan. Proses ini sulit dilakukan dengan switch tradisional, sebab logika control untuk setiap switch terletak dalam logika switching yang sama. Proses pengelolaan jaringan, tingkat QoS (*Quality of Service*) dan tingkat keamanan dapat sangat memakan waktu jika jaringan perusahaan yang besar yang menggunakan perangkat jaringan dari beberapa vendor, sebab administrator jaringan harus mengkonfigurasi peralatan masing-masing vendor secara terpisah dan menyesuaikan kinerja serta parameter-parameternya [10].





Penerapan VLAN ini sangat bermanfaat untuk pengembangan jaringan dalam ruang lingkup local area dan untuk dari segi pembagian IP address juga dapat di konfigurasi sesuai kebutuhan. Selain dari sisi yang sudah disebutkan VLAN juga aman dari segi keamanan jaringan karena tidak semua segmen IP sama antara VLAN. Kemudian dari sisi traffic data juga VLAN dapat di monitoring agar traffic bisa terlihat oleh administrator dan langsung mengambil keputusan untuk menambah jaringan atau memperkecil ruang lingkup jaringan local [11].

### 2.2. Trunk Link

Metode Trunk link merupakan perintah yang digunakan untuk mengaktifkan port switch sebagai jembatan beberapa VLAN ID untuk digunakan sebagai penghubung VLAN ID yang sama pada perangkat switch yang berbeda. Parameter perintah Trunk link yang digunakan adalah :

Tabel 1. Perintah Trunk Link

<i>Perintah</i>	<i>Arti/Maksud</i>	<i>Keterangan</i>
Switcport	Mengatur karakteristik mode peralihan	Memungkinkan perangkat atau port pada switch untuk mengirim dan menerima paket serta berkomunikasi dengan perangkat lain.
Mode	Mengatur jenis trunking perangkat	Port switch yang ingin dihubungkan menggunakan atau caranya atau jenis koneksinya.
Trunk	Mengatur jenis trunking ke Trunk tanpa syarat	Sebagai jembatan beberapa VLAN ID agar terhuubung pada switch yang berbeda dengan VLAN ID yang sama.
Allowed	Menetapkan karakteristik VLAN yang diperbolehkan saat interface dalam mode trunking	Menetapkan akses pada VLAN ID menggunakan port sebagai penghubung VLAN ID yang sama.
VLAN	Virtualisasi LAN	Jenis virtual yang menjaga broadcast domain pada satu buah ID.
All	Semua VLAN ID	Memberikan akses pada beberapa VLAN ID menggunakan port sebagai penghubung VLAN ID yang sama.

Berdasarkan perintah tersebut diatas trunk link mempunyai keunggulan jika dilihat dari ketersediaan perangkat, artinya hemat dalam menggunakan perangkat jaringan khususnya port pada switch. Ini dikarenakan cukup dengan satu buah port dan satu buah koneksi jaringan kabel yang menghubungkan 2 buah switch dapat digunakan sebagai jembatan penghubung beberapa VLAN ID bisa lebih dari satu buah VLAN ID agar terkoneksi dengan VLAN ID sama dengan switch yang berbeda. Tetapi ada kendala dibalik kelebihan metode ini, yaitu dikarenakan hanya mengandalkan satu buah koneksi port atau kabel jika terjadi down atau off port atau kabel tersebut maka beberapa VLAN ID yang melewati jembatan tersebut akan mengalami putus koneksi dengan VLAN ID yang sama pada switch yang berbeda.

### 2.2 Access Link

Metode access link ini sama dengan perintah yang digunakan untuk memasukkan port switch ke dalam VLAN ID atau dapat juga digunakan sebagai jembatan penghubung satu buah VLAN ID agar dapat berkomunikasi dengan VLAN ID yang sama pada switch yang berbeda. Parameter perintah Access Link yang digunakan adalah :

Tabel 2. Perintah Access Link

<i>Perintah</i>	<i>Arti/Maksud</i>	<i>Keterangan</i>
-----------------	--------------------	-------------------



DOI: 10.52362/jisicom.v8i2.1663

Ciptaan disebarluaskan di bawah [Lisensi Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/).

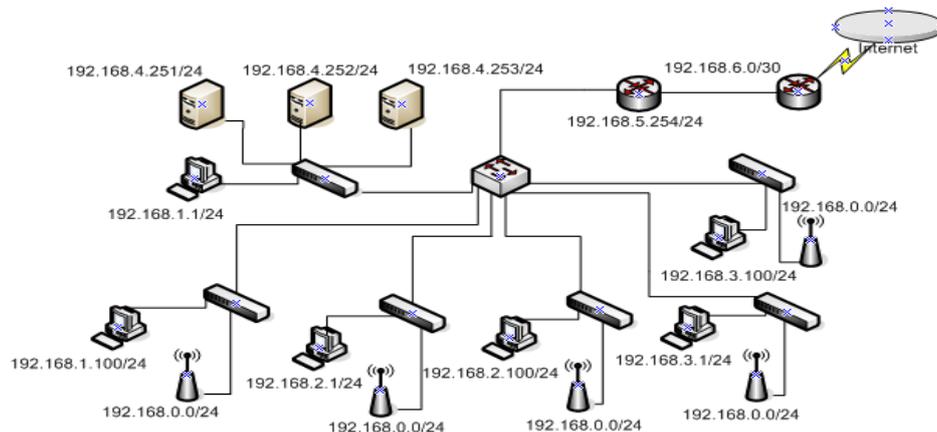
Switcport	Port yang ada didalam switch	Memungkinkan perangkat atau port pada switch untuk mengirim dan menerima paket serta berkomunikasi dengan perangkat lain.
Mode	Cara atau Jenis	Port switch yang ingin dihubungkan menggunakan atau caranya atau jenis koneksinya.
Access	Mengatur jenis trunking ke Access tanpa syarat	Sebagai Koneksi atau jembatan satu buah VLAN ID yang sama.
VLAN	Virtualisasi LAN	Jenis virtual yang menjaga broadcast domain pada satu buah ID.

Sesuai perintah yang digunakan pada Access Link merupakan perintah yang digunakan mempunyai dua fungsi, yaitu :

1. Perintah Access Link digunakan untuk memasukkan atau menseting atau memindahkan port yang ada didalam switch dipindahkan ke dalam VLAN ID selain VLAN 1, dan sebenarnya secara default switch manageable yang digunakan untuk membuat VLAN, bahwa semua port yang ada didalam switch tersebut sudah masuk atau berada pada VLAN 1 dengan nama VLAN default.
2. Perintah Access Link ini juga dapat digunakan sebagai trunking atau jembatan penghubung dengan dua switch yang berbeda, tetapi jembatan yang digunakan dengan metode access link ini hanya dapat dilewati oleh satu buah VLAN ID saja tidak bias lebih.

Berdasarkan keterangan diatas maka dapat disimpulkan bahwa metode access link secara efisiensi maintenance atau pemeliharaan tidak terlalu sulit, tetapi secara efisiensi perangkat atau khususnya jumlah port yang digunakan akan boros sekali, ini dikarenakan setiap jembatan VLAN ID yang berbeda memerlukan satu buah koneksi fisik kabel dan port pada switch. Dapat disimpulkan bahwa jumlah VLAN ID pada jaringan LAN akan berbanding lurus dengan kebutuhan port switch.

### III. PEMBAHASA DAN HASIL



Gambar 1. Skema Berjalan

Terdapat sebuah skema jaringan dengan keterangan sebagai berikut : Switch Catalist (SC2 sampai dengan SC7) dan Switch Multilayer (SC1) yang berada disekitar skema jaringan berjalan. Switch catalist ini digunakan untuk membuat VLAN pada jaringan, sehingga semua perangkat jaringan computer seperti PC, Server dan Akses Point



DOI: 10.52362/jisicom.v8i2.1663

Ciptaan disebarluaskan di bawah [Lisensi Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/).



berada didalam VLAN nantinya. Sedangkan Switch Multilayer merupakan switch core atau pusat koneksi dari switch catalyst yang ada didalam skema jaringan berjalan tersebut. Switch catalyst berjumlah 6 (enam) perangkat sedangkan Switch Multilayer berjumlah 1 (satu) perangkat Switch Multilayer (SC1). Berikut ini table gambaran koneksi port-port pada switch catalyst dan switch multilayer pada skema jaringan berjalan, yaitu :

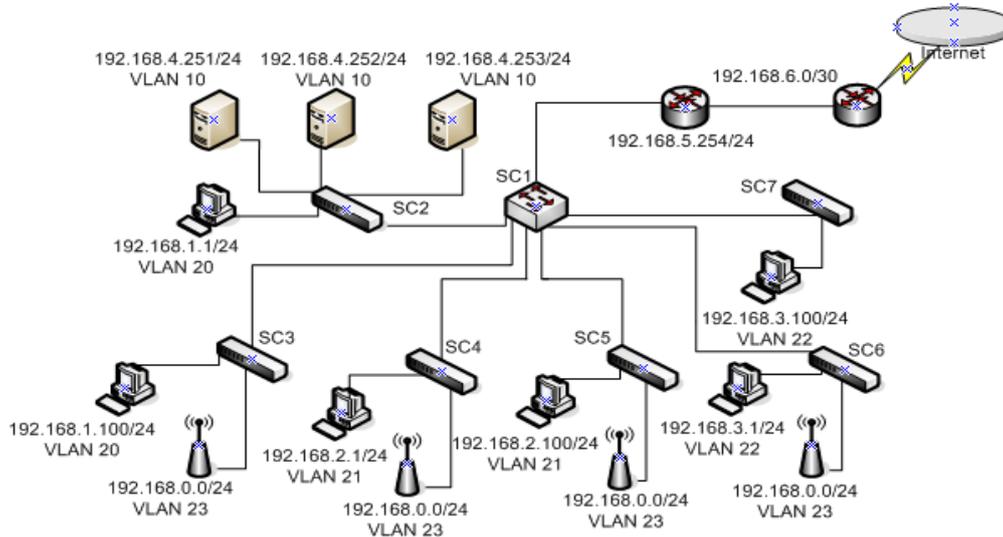
Tabel 3. Connectivity Switch ke Seluruh perangkat jaringan

<i>Nama Perangkat</i>	<i>Menggunakan Port</i>	<i>Terhubung</i>	<i>Keterangan</i>
Switch Multilayer (SC1)	FastEthernet 0/1	SC2	SC2 terletak Lant 6
	FastEthernet 0/2	SC3	SC3 terletak Lant 5
	FastEthernet 0/3	SC4	SC4 terletak Lant 5
	FastEthernet 0/4	SC5	SC5 terletak Lant 7
	FastEthernet 0/5	SC6	SC6 terletak Lant 7
	FastEthernet 0/6	SC7	SC7 terletak Lant 7
	GigaEthernet 0/1	Router	Router terletak Lant 6
Switch Catalist (SC2)	GigaEthernet 0/1	SC1	Lant 6
	FastEthernet 0/2	PC 1	Lant 6
	FastEthernet 0/11	Server Aplikasi 1	Lant 6
	FastEthernet 0/12	Server Aplikasi 2	Lant 6
	FastEthernet 0/13	Server Aplikasi 3	Lant 6
Switch Catalist (SC3)	GigaEthernet 0/1	SC1	Lant 6
	GigaEthernet 0/2	Akses Point	Lant 5
	FastEthernet 0/1 ...	PC-PC Lant 7	Lant 5
Switch Catalist (SC4)	GigaEthernet 0/1	SC1	Lant 5
	GigaEthernet 0/2	Akses Point	Lant 5
	FastEthernet 0/1 ...	PC-PC Lant 5	Lant 5
Switch Catalist (SC5)	GigaEthernet 0/1	SC1	Lant 6
	GigaEthernet 0/2	Akses Point	Lant 7
	FastEthernet 0/1 ...	PC-PC Lant 7	Lant 7
Switch Catalist (SC6)	GigaEthernet 0/1	SC1	Lant 6
	GigaEthernet 0/2	Akses Point	Lant 7
	FastEthernet 0/1 ..	PC-PC Lant 7	Lant 7
Switch Catalist (SC7)	GigaEthernet 0/1	SC1	Lant 6
	FastEthernet 0/1...	PC-PC Lant 7	Lant 7

### 3.1. Optimalisasi VLAN dengan Trunk Link

Skema jaringan berjalan mengalami perubahan saat diterapkan VLAN dengan menerapkan *trunking* atau VTP (*Virtual Trunking Protokol*) untuk semua VLAN, fungsinya agar semua VLAN dengan ID yang sama dapat terhubung satu sama lainnya di perangkat switch yang berbeda. Digunakan juga metode Inter-VLAN pada perangkat Switch Multilayer SC1 yang berfungsi menghubungkan beberapa VLAN ID yang berbeda, kebutuhan koneksi ini dikarenakan kebutuhan komunikasi dengan server-server yang ada didalam skema jaringan berjalan. Dibawah ini gambar tentang perubahan skema jaringan berjalan.





Gambar 2 Skema Usulan Metode Trunk untuk VLAN

Kebutuhan akan adanya routing terhadap metode inter-VLAN agar semua VLAN ID yang berbeda ada didalam jaringan dapat terhubung, maka setiap perangkat jaringan yang masuk ke dalam VLAN ID harus mempunyai gateway yang akan difungsikan sebagai gerbang komunikasi VLAN yang berbeda-beda agar dapat terhubung satu sama lainnya. Metode Inter-VLAN juga menggunakan teknik yang dikenal dengan SVI (*Sub VLAN Interface*), dengan adanya SVI ini VLAN ID yang ada didalam jaringan akan mempunyai gateway berupa IP address. Dan IP address yang diinputkan didalam SC1 akan dijadikan gateway dan diinputkan ke seluruh perangkat jaringan yang berada didalam VLAN tersebut. Didalam menentukan IP Address SVI yang nantinya sebagai gateway pada setiap VLAN ID tinggal mengikuti Network ID dan Host ID yang ada di setiap VLAN ID tersebut. Dan SVI yang digunakan adalah sebagai berikut :

Tabel 4. SVI sebagai Gateway Perangkat VLAN ID

SVI	VLAN ID	Keterangan
192.168.4.254/24	VLAN 10	Gateway dari 3 Server
192.168.1.254/24	VLAN 20	Gateway dari PC-PC lant 6
192.168.2.254/24	VLAN 21	Gateway dari PC-PC lant 5
192.168.3.254/24	VLAN 23	Gateway dari PC-PC lant 7
192.168.0.254/24	VLAN 23	Gateway dari AP lant 5, 6 dan 7

Selanjutnya konfigurasi koneksi fisik kabel dan port switch yang digunakan VLAN-VLAN yang ada didalam jaringan computer pada Switch Multilayer (SC1) yang terhubung ke semua perangkat switch catalyst (SC2 sampai dengan SC7):

Tabel 5. Connection Port Metode Trunk Link

SC 1 Port	Hubungan	Metode Link	Keterangan
FastEthernet 0/1	SC2 GigaEthernet 0/1	Trunk link	VLAN 10 dan VLAN 20
FastEthernet 0/2	SC3 GigaEthernet 0/1	Trunk link	VLAN 20 dan VLAN 23
FastEthernet 0/3	SC4 GigaEthernet 0/1	Trunk link	VLAN 21 dan VLAN 23



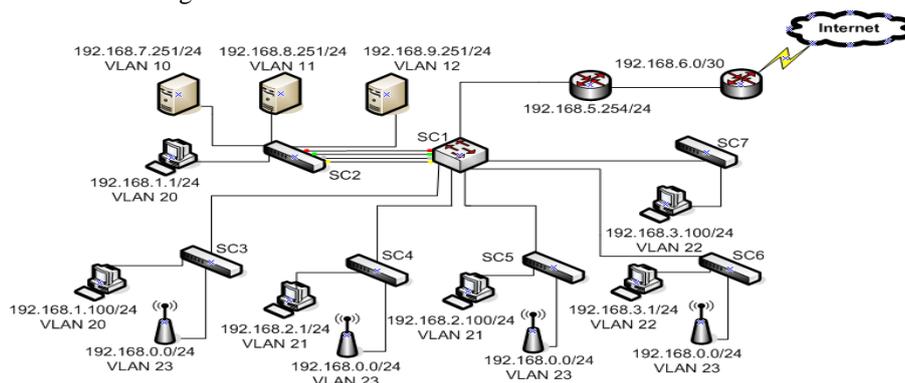
FastEthernet 0/4	SC5 GigaEthernet 0/1	Trunk link	VLAN 21 dan VLAN 23
FastEthernet 0/5	SC6 GigaEthernet 0/1	Trunk link	VLAN 22 dan VLAN 23
FastEthernet 0/6	SC7 GigaEthernet 0/1	Trunk link	VLAN 22 dan VLAN 23

Didalam trunking metode *Trunk Link* terjadi permasalahan ini dikarenakan jika sebuah port atau jalur fisik kabel yang digunakan mengalami *connection failure* atau *down* yang disebabkan lingkungan atau bisa saja umur port, atau bisa juga kemampuan hardware atau bisa saja alam seperti (terkena petir, atau konslet dan lain-lainnya). Ini akan menyebabkan jalur VLAN-VLAN ID yang melalui port atau jalur koneksi kabel tersebut akan mengalami *connection failure* atau *down*. Contohnya saja dilihat dari table *Connection Port* trunking Metode Trunk Link pada port FastEthernet 0/1 SC1 mengalami *connection failure* atau *down*, maka VLAN 10 yang didalamnya terdapat koneksi 3 server (Server Aplikasi 1, Server Aplikasi 2 dan Server Aplikasi 3) dan VLAN 20 dengan berisi satu buah PC di lantai 6 tidak akan bisa diakses oleh semua computer atau perangkat jaringan yang ada didalam jaringan tersebut, tetapi PC-PC dan Akses Point yang berada di SC 3 dengan VLAN 20 ini tetap akan terkoneksi dengan semua VLAN ID yang ada didalam jaringan.

Seorang administrator jaringan yang mempunyai tugas dan fungsinya bertanggung jawab atas kelancaran konektivitas jaringan computer atau VLAN-VLAN yang ada didalam skema jaringan yang berjalan pada sebuah organisasi atau perusahaan. Mempertimbangkan metode lainnya untuk menanggulangi atau meminimalisir permasalahan ini. Artinya seorang administrator harus berfikir bagaimana mengatasi atau meminimalisir permasalahan agar semua perangkat server didalam jaringan dapat berjalan baik ataupun jika terjadi permasalahan *connection failure* pada jalur koneksi VLAN di port switch atau koneksi fisik kabel tersebut terjadi, ini tidak melibatkan semua server mengalami *connection failure* cukup satu server saja yang mengalami hal tersebut. Dan dalam hal tindakan perbaikan permasalahan ini dapat diidentifikasi dengan efektif dan melakukan pemulihan secara cepat.

Dalam hal meminimalisir permasalahan tersebut jika terjadi, sebaiknya setiap server berada pada VLAN ID yang berbeda, dan port switch yang difungsikan sebagai trunking bertanggung jawab pada satu koneksi VLAN ID terhubung ke semua VLAN yang ada didalam skema jaringan. Maka didalam koneksi perangkat-perangkat server menggunakan trunking metode *Access Link* untuk dapat terhubung ke semua VLAN yang ada didalam skema jaringan tersebut. Dan untuk lebih meminimalisir terjadi *connection failure* yang besar, sebaiknya setiap server mempunyai VLAN ID yang berbeda satu sama lainnya dan harus memiliki IP Address dengan network id yang berbeda-beda.

### 3.2. Optimalisasi VLAN dengan Access Link

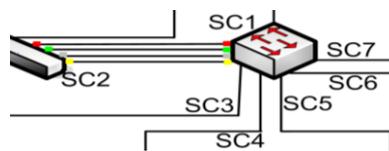


Gambar 3. Skema Usulan Metode Access Link untuk VLAN



Gambar diatas merupakan skema usulan yang menambahkan trunking untuk jalur koneksi 3 perangkat server, konektivitas antara SC2 dengan SC1, antara lain adalah :

1. Menambahkan jalur fisik dan port yang digunakan sebagai *trunking* oleh kedua switch tersebut sebagai *Access Link* untuk VLAN-VLAN Server. agar kinerja atau *conecctivity* VLAN-VLAN server yang ada didalam jaringan dapat terus terjaga.
2. Ketiga server dibedakan VLAN ID nya, tidak dijadikan satu VLAN ID.
3. Memberikan IP Address pada setiap server dengan network id yang berbeda satu sama lainnya, dan nantinya harus memiliki gateway pada setiap server tersebut, gateway yang dimiliki oleh ketiga server tersebut berbeda pula network id nya satu sama lainnya.
4. Karena terdapat PC dalam SC2, maka PC VLAN 20 tersebut harus mempunyai jalur fisik kabel atau port switch tersendiri atas ketiga perangkat server.



Gambar 4. Port Connectivity SC1 ke SC2 dan ke Semua Switch

Tabel 6. Connection Port Metode Access Link dan Trunk Link

SC 1 Port	Hubungan	Metode Link	Keterangan
FastEthernet 0/1	SC2 GigaEthernet 0/1	-	Tidak digunakan
FastEthernet 0/10	SC2 FastEthernet 0/20	Access link	VLAN 10 atau Server 1
FastEthernet 0/11	SC2 FastEthernet 0/21	Access link	VLAN 11 atau Server 2
FastEthernet 0/12	SC2 FasEthernet 0/22	Access link	VLAN 12 atau Server 3
FastEthernet 0/7	SC2 GigaEthernet 0/1	Access link	VLAN 20
FastEthernet 0/2	SC3 GigaEthernet 0/1	Trunk link	VLAN 20 dan VLAN 23
FastEthernet 0/3	SC4 GigaEthernet 0/1	Trunk link	VLAN 21 dan VLAN 23
FastEthernet 0/4	SC5 GigaEthernet 0/1	Trunk link	VLAN 21 dan VLAN 23
FastEthernet 0/5	SC6 GigaEthernet 0/1	Trunk link	VLAN 22 dan VLAN 23
FastEthernet 0/6	SC7 GigaEthernet 0/1	Trunk link	VLAN 22 dan VLAN 23

```

SCI#sh vlan br
VLAN Name      Status      Ports
-----
1    default      active     Fa0/1, Fa0/3, Fa0/4, Fa0/5
      Fa0/6, Fa0/8, Fa0/9, Fa0/13
      Fa0/14, Fa0/15, Fa0/16, Fa0/17
      Fa0/18, Fa0/19, Fa0/20, Fa0/21
      Fa0/22, Fa0/23, Fa0/24, Gig0/1
      Gig0/2
10   Server       active     Fa0/10
11   Server2     active     Fa0/11
12   Server3     active     Fa0/12
20   Client1     active     Fa0/7
21   Client2     active
22   Client3     active
23   AP          active
1002 fddi-default active
1003 token-ring-default active
  
```

Gambar 5. Acces Link VLAN pada SC1



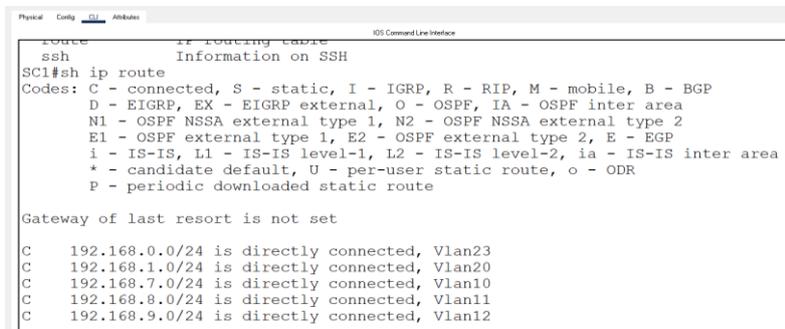
DOI: 10.52362/jisicom.v8i2.1663

Ciptaan disebarluaskan di bawah [Lisensi Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/).

Selanjutnya konfigurasi routing yang ada didalam SC1 untuk VLAN-VLAN yang ada didalam jaringan computer agar dapat terhubung satu sama lainnya yang memiliki VLAN ID berbeda.

Tabel 7. SVI sebagai Gateway Perangkat VLAN ID

SVI	VLAN ID	Keterangan
192.168.4.254/24	-	Tidak digunakan lagi
192.168.7.254/24	VLAN 10	Gateway dari Server 1
192.168.8.254/24	VLAN 11	Gateway dari Server 2
192.168.9.254/24	VLAN 12	Gateway dari Server 3
192.168.1.254/24	VLAN 20	Gateway dari PC-PC lant 6
192.168.2.254/24	VLAN 21	Gateway dari PC-PC lant 5
192.168.3.254/24	VLAN 23	Gateway dari PC-PC lant 7
192.168.0.254/24	VLAN 23	Gateway dari AP lant 5, 6 dan 7



```

IOS Command Line Interface
-----
Route
ssh
Information on SSH
SC1#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.0.0/24 is directly connected, Vlan23
C    192.168.1.0/24 is directly connected, Vlan20
C    192.168.7.0/24 is directly connected, Vlan10
C    192.168.8.0/24 is directly connected, Vlan11
C    192.168.9.0/24 is directly connected, Vlan12
  
```

Gambar 6. Routing Sub-VLAN Inetrface pada SC1

Pada penelitian ini berfokus pada meminimalisir *connection failure* atau *down* sebuah port yang digunakan sebagai koneksitas *trunking* yang digunakan untuk VLAN-VLAN agar terjadi pengurangan terhadap VLAN yang mengalami *connection failure* atau *down* tersebut. Pengujian terhadap *connection failure* terjadi pada VLAN 10, VLAN 11 dan VLAN 12 dibawah ini :

Tabel 8. SC1 FastEthernet 0/10 terjadi Connection Failure

VLAN	Connection	Status
VLAN 20	Server 1	Connection failure
VLAN 20	Server 2	Connect
VLAN 20	Server 3	Connect
VLAN 21	Server 1	Connection failure
VLAN 21	Server 2	Connect
VLAN 21	Server 3	Connect
VLAN 22	Server 1	Connection failure
VLAN 22	Server 2	Connect
VLAN 22	Server 3	Connect
VLAN 23	Server 1	Connection failure
VLAN 23	Server 2	Connect
VLAN 23	Server 3	Connect





Didalam table diatas pengujian dilakukan jika terjadi connection failure pada switch SC1 dengan port FastEthernet 0/10 sebagai *trunking* yang menggunakan metode “*Access Link*” ke Server aplikasi 1 terhubung ke VLAN-VLAN yang ada didalam jaringan. Dikarenakan mengalami *connection failure* pada jalur *trunking access link* untuk server aplikasi 1 ini, maka server tersebut tidak dapat terhubung ke VLAN-VLAN yang ada didalam jaringan. Sedangkan VLAN 11 berisi sever aplikasi 2 dan VLAN 12 berisi server aplikasi 3 masih tetap terhubung ke VLAN-VLAN yang ada didalam jaringan tersebut.

Begitu sebaliknya jika switch SC1 dengan port FastEthernet 0/11 sebagai *trunking* yang menggunakan metode “*Access Link*” ke Server aplikasi 2 terhubung ke VLAN-VLAN yang ada didalam jaringan. Dikarenakan mengalami *connection failure* pada jalur *trunking access link* untuk server aplikasi 2 ini, maka server tersebut tidak dapat terhubung ke VLAN-VLAN yang ada didalam jaringan. Sedangkan VLAN 10 berisi sever aplikasi 1 dan VLAN 12 berisi server aplikasi 3 masih tetap terhubung ke VLAN-VLAN yang ada didalam jaringan tersebut.

#### IV. KESIMPULAN

Ketersediaan perangkat-perangkat jaringan yang ada jika menggunakan metode *Access Link*, akan menyebabkan kebutuhan port-port yang tersedia pada switch. Sehingga jika penerapan *Access Link* pada VLAN ini diterapkan didalam semua switch maka kebutuhan akan adanya port pada switch akan bertambah dan otomatis akan adanya banyaknya switch yang tersedia pada jaringan tersebut. Ini dikarenakan setiap VLAN ID yang ada didalam jaringan tersebut membutuhkan satu port switch. Sehingga jika didalam jaringan terdapat 6 (enam) VLAN ID maka minimal 6 port pada switch harus disediakan dan ini belum termasuk kebutuhan perangkat-perangkat jaringan lainnya akan ketersediaan port switch tersebut, contohnya PC, router, modem printer server dan akses point. Sehingga tidak efisien jika dilihat dari kebutuhan perangkat yang akan digunakan dengan menggunakan metode “*Access Link*”.

Pertimbangan selanjutnya berdasarkan adanya terjadi “*connection failure*” atau *down* pada port switch yang digunakan sebagai *Trunk Link* maka akan terjadi *connection failure* secara masal dan bersamaan terhadap VLAN-VLAN yang berada pada jalur koneksi port switch tersebut. Kejadian ini amat sangat merugikan untuk kegiatan bisnis pada sebuah organisasi.

Maka betapa penting dalam melakukan kombinasi metode *Trunk Link* dan *Access Link* agar kinerja VLAN-VLAN yang ada didalam jaringan tetap berjalan. Kedua metode ini hanya dapat melakukan minimalis *connection failure* yang terjadi pada hubungan VLAN didalam jaringan computer. Sebagai rekomendasi penelitian selanjutnya untuk membuat jalur backup terhadap *connection failure* pada VLAN ini agar digunakan metode STP (*Spanning Tree Protocol*), didalam metode ini pada switch menggunakan dua metode connectivity *Trunk Link* dan *Access Link* dan selanjutnya agar tidak terjadi loop packet data pada switch.

Memberikan pernyataan bahwa apa yang diharapkan, seperti yang dinyatakan dalam "Pendahuluan" akhirnya dapat mengakibatkan "Hasil dan Diskusi", sehingga ada kemampuan. Selain itu dapat juga ditambahkan prospek pengembangan hasil penelitian dan prospek penerapan studi lanjutan. Kesimpulan harus menjawab tujuan dari penelitian. Menggunakan kalimat yang tidak terlalu panjang, lebih padat dan fokus

#### REFERENASI

- [1] A. Fitriansyah, A. Andreansyah, and A. Sopian, “Penerapan Static VLAN Dan Access List Untuk Meningkatkan Keamanan Jaringan,” *J. Teknol. Inform. dan Komput.*, vol. 5, no. 2, pp. 58–63, 2019, doi: 10.37012/jtik.v5i2.176.
- [2] Y. Pantu, C. Iswahyudi, and R. Y. R. Kusumaningsih, “ANALISIS DAN PERANCANGAN VLAN PADA DISHUBKOMINFO KABUPATEN MANGGARAI MENGGUNAKAN CISCO PACKET TRACER,” *J. JARKOM*, vol. 3, no. 1, pp. 62–72, 2015.
- [3] I. P. A. Pratama, *Handbook Jaringan Komputer.pdf*. Bandung: Informatika Bandung, 2014.
- [4] A. S. Hidayat, S. Sobari, B. O. Lubis, and P. M. Akhrianto, “Connetivity Jaringan Public Dengan Satu ISP





- Menghubungkan Kantor Cabang Dengan Menggunakan Metode Metro Ethernet,” *J. Teknol. Inform. dan Komput.*, vol. 6, no. 2, pp. 63–73, 2020, doi: 10.37012/jtik.v6i2.288.
- [5] A. S. Hidayat, A. Salim, Y. I. Maulana, and P. M. Akhirianto, “Penggunaan Firewall Metode Access Control List Sebagai Blok Situs dan Fitering File Transfer Protocol pada PT Indoraya Makmur Abadi,” vol. 10, no. 2, pp. 584–601, 2024.
- [6] K. Nugroho, “Pengaruh Native VLAN terhadap Overhead Trafik Data pada Jaringan LAN,” *ELKOMIKA J. Tek. Energi Elektr. Tek. Telekomun. Tek. Elektron.*, vol. 9, no. 2, pp. 404–414, 2021, doi: 10.26760/elkomika.v9i2.404.
- [7] A. A. Putra, I. Ispandi, and B. O. Lubis, “Perancangan Firewall dan Spanning Tree Protocol Sebagai Sistem Keamanan Jaringan Komputer,” *J. Teknol. Inform. dan Komput.*, vol. 9, no. 1, pp. 48–60, 2023, doi: 10.37012/jtik.v9i1.1340.
- [8] J. S. Beasley and P. Nilkaew, *A Practical Guide to Advanced Networking Third Edition*. Indianapolis, Indiana: Pearson, 2013.
- [9] S. Iwan, “Cisco CCNA dan Jaringan Komputer,” *Bandung: Informatika Bandung*. Informatika Bandung, Bandung, pp. 1–248, 2010.
- [10] O. Coker and S. Azodolmolky, *Software Define Network With OpenFlow.pdf*, Second Edi. Birmingham: Packt Publishing, 2017.
- [11] M. Ryansyah, “Perancangan Virtual LAN Menggunakan Switch Manajemen Dengan Mikrotik,” *J. Tek. Komput. AMIK BSI*, vol. 4, no. 1, pp. 17–20, 2018.

