JURNAL DEVICE, VOL. 15 NO 2, November 2025, 250-260
ISSN: 0216-9185 | eISSN: 2746-8984

PERANCANGAN JARINGAN VIRTUAL LOCAL AREA NETWORK (VLAN) TRUNKING UNTUK ISOLASI BEDA DIVISI DENGAN SWITCH CISCO PADA KPID DKI JAKARTA

Fezan Nabawi[(1)], Juliyanto[(2)], Mohammad Reza Fahlevi[(3)]

[1,2,3)] Universitas Nahdlatul Ulama Indonesia
Email : fezan@unusia.ac.id [1)], juli91170@gmail.com, [2)] rezafah@unusia.ac.id [3)]

ABSTRAK

Penelitian ini bertujuan untuk merancang dan mengimplementasikan jaringan komputer dengan menerapkan teknologi Virtual Local Area Network (VLAN) trunking guna meningkatkan segmentasi, dan keamanan dalam suatu sistem jaringan. Dalam era digital saat ini, kebutuhan akan jaringan yang aman dan terstruktur menjadi semakin penting, terutama di lingkungan kerja yang melibatkan banyak divisi atau departemen. Penerapan VLAN memungkinkan pemisahan logis antar perangkat dalam satu jaringan fisik, sehingga komunikasi data dapat diatur lebih terarah dan terjaga dari akses yang tidak diinginkan. Penelitian ini menggunakan Switch Cisco sebagai alat bantu implementasi VLAN. Proses pengujian dilakukan dengan mengirimkan paket ICMP antar perangkat dalam VLAN yang sama maupun berbeda. Hasil pengujian menunjukkan bahwa komunikasi antar perangkat dalam VLAN yang sama berhasil dilakukan tanpa hambatan, sedangkan komunikasi antar VLAN yang berbeda secara default dibatasi, kecuali apabila dilakukan konfigurasi routing antar VLAN. Hal ini menandakan bahwa pengaturan segmentasi berjalan efektif. Selain itu, pengujian juga menunjukkan bahwa jaringan memiliki performa yang baik dengan latensi rendah dan koneksi yang stabil. Dengan demikian, penerapan VLAN dan trunking terbukti dapat membangun jaringan yang lebih efisien, aman, dan mudah dikelola.

Kata Kunci: VLAN,Trunking, Switch Cisco.

ABSTRACT

This research aims to design and implement a computer network by applying Virtual Local Area Network (VLAN) technology and trunking configuration to enhance segmentation, and security within a network system. In today's digital era, the need for a secure and structured network is increasingly important, especially in work environments involving multiple divisions or departments. The implementation of VLAN enables logical separation between devices within a single physical network, allowing data communication to be more directed and protected from unauthorized access. This study uses Cisco Switch as a tool for VLAN implementation. Testing was conducted by sending ICMP packets between devices within the same VLAN and across different VLANs. The test results show that communication between devices within the same VLAN was successful and uninterrupted, while communication across different VLANs was restricted by default unless inter-VLAN routing was configured. This indicates that the segmentation setup works effectively. Furthermore, the network demonstrated good performance with low latency and stable connections during testing. Thus, the implementation of VLAN and trunking proves to be an effective approach in building a more efficient, secure, and manageable network.

Keywords: VLAN, Trunking, Cisco Switch

1. PENDAHULUAN

Kemajuan teknologi informasi telah mendorong berbagai organisasi untuk memanfaatkan infrastruktur jaringan yang lebih andal dan efisien guna mendukung kegiatan operasional. Di lembaga seperti Komisi Penyiaran Indonesia (KPI) Daerah Jakarta, yang terdiri dari beberapa departemen dengan tanggung jawab dan fungsi yang beragam, tantangan manajemen jaringan seringkali muncul. Masalah seperti kebocoran data antar departemen, penurunan kinerja jaringan akibat konflik lalu lintas, serta kesulitan dalam memantau dan mengelola jaringan merupakan kendala yang harus segera diatasi. Oleh karena itu, penerapan teknologi VLAN (*Virtual Local Area Network*) sangat penting untuk isolasi lalu lintas antar departemen yang efektif.(Elimanafe ,dkk., 2022)

Untuk mendukung operasional dan mencegah akses tanpa izin, pemisahan diperlukan untuk mengisolasi lalu lintas antar divisi. Teknologi VLAN merupakan solusi ideal untuk implementasi di KPID DKI Jakarta karena memungkinkan isolasi lalu lintas data antar departemen dalam jaringan fisik yang sama. Dengan menggunakan *VLAN trunking*, lalu lintas data dari setiap departemen dapat dipisahkan secara logistik, meningkatkan keamanan dan mencegah interferensi antar departemen. Lebih lanjut, VLAN mengoptimalkan pemanfaatan *bandwidth* dengan membatasi dan mengurangi lalu lintas yang tidak perlu, dan meningkatkan kinerja jaringan. Implementasi VLAN berbasis *switch Cisco* dengan protokol IEEE 802.1Q memastikan stabilitas konfigurasi jaringan, serta memudahkan pengelolaan dan pemantauan lalu lintas antar departemen. Hal ini membuat jaringan di KPID DKI Jakarta lebih terorganisir, aman, dan efisien.(Rahman ,dkk., 2020)

VLAN memungkinkan jaringan fisik dibagi menjadi beberapa jaringan tanpa memerlukan perangkat keras tambahan. Fitur ini mengisolasi lalu lintas antar departemen, mencegah akses tidak sah dari departemen lain. Hal ini tidak hanya meningkatkan keamanan jaringan tetapi juga mengoptimalkan kinerja jaringan. Lebih lanjut, VLAN menyederhanakan manajemen bagi organisasi dengan kebutuhan lalu lintas jaringan yang kompleks. *Switch Cisco* merupakan salah satu perangkat yang mendukung implementasi VLAN dan kemampuannya untuk mendukung fitur-fitur seperti *VLAN trunking*, dan seterusnya.

Studi ini mengkaji VLAN dan *switch Cisco*, yang telah menunjukkan keberhasilan dalam berbagai skenario. Sebagai contoh, menurut Pirzi Kurniawan (2022), VLAN memungkinkan partisi jaringan yang hemat biaya menjadi beberapa bagian terpisah, dan penggunaan *VLAN Trunking Protocol (VTP)* akan memudahkan administrator jaringan untuk mengelola dan mengatur VLAN yang ada. Menurut Widyastuti & Hendrian (2022), permasalahannya adalah kemudahan orang dari departemen lain yang tidak memiliki izin untuk mengakses atau melihat berkas rahasia milik departemen tertentu. Oleh karena itu, implementasi VLAN diperlukan untuk membatasi akses antar pengguna jaringan komputer guna menjaga keamanan dan autentikasi data dan berkas. Lebih lanjut, Elimanafe dkk. (2022) juga menemukan bahwa VLAN (Virtual Area Network) dapat meningkatkan kinerja jaringan, partisi jaringan, dan menyederhanakan manajemen berdasarkan regulasi tertentu.

Melihat kebutuhan Komisi Penyiaran Indonesia Daerah DKI Jakarta yang membutuhkan jaringan dengan keamanan tinggi dan pengelolaan trafik yang optimal antar divisi, penelitian ini penting di lakukan untuk merancang jaringan *VLAN Trunking* berbasis *Switch Cisco* diharapkan mampu memberikan solusi yang terstruktur untuk mengisolasi trafik antar divisi, meningkatkan performa jaringan, dan memberikan panduan teknis yang dapat langsung diimplementasikan. Selain itu, penelitian ini juga di harapkan dapat menjadi referensi bagi organisasi lain yang memiliki kebutuhan serupa.

2. METODE

Tempat dan Waktu Penelitian Kegiatan penelitian ini dilakukan di Komisi Penyiaran Indonesia Daerah (KPID) DKI Jakarta

Jenis penelitian yang dilakukan menggunakan metode kualitatif, dengan melakukan teknik pengumpulan data sebagai berikut:

a. **Observasi**

Observasi (Pengamatan Langsung) Adapun pengamatan langsung dilakukan di kantor KPID Jakarta

b. **Wawancara**

Digunakan untuk mengetahui lebih detail terkait permasalahan yang terjadi pada perusahaan. Dan wawancara dilakukan secara langsung kepada Staff perusahaan.

c. **Studi Pustaka**

Menelaah terhadap buku, jurnal, catatan-catatan dan laporan yang ada hubungannya dengan masalah yang dipecahkan.

Pada implementasi perancangan ini secara sistem perangkat yang digunakan adalah sebagai berikut:

2.1. Hardware (Perangkat Keras)**,** yang digunakan:

2.1.1. Laptop dengan spesifikasi sebagai berikut:

- Processor: Intel Core i5
- RAM: 8 GB untuk mendukung kelancaran simulasi jaringan kompleks
- Storage: SSD 256 GB
- Monitor: Resolusi HD untuk menampilkan secara visual

2.1.2. *Switch Cisco Catalyst 2960*

Tipe: Fixed-configuration Layer 2 switch, jumlah Port:

- 24 port Ethernet 10/100 Mbps
- 2 port tambahan 10/100/1000 Mbps uplink (RJ-45 atau SFP)
- Throughput: 6.5 Mpps (million packets per second)
- Switching capacity (*Bandwidth*): 16 Gbps
- Layer Support: Layer 2 switching (VLAN, Trunking, STP)
- VLAN Support: Hingga 255 VLAN aktif (ID VLAN 1–4094)
- Power Supply: Internal (AC input)
- Manajemen: CLI (Command Line Interface) via console, Telnet, atau SSH.
- Port security
- 802.1x authentication
- Access Control List (ACL) dasar
- Fitur QoS: Mendukung Quality of Service untuk mengatur prioritas trafik
- Ukuran Fisik: 1RU (rack unit)

2.1.3. Komputer Client

Beberapa komputer client digunakan oleh pengguna akhir dalam jaringan. Komputernya memiliki spesifikasi sebagai berikut:

- Prosesor: Intel Core i3/i5 generasi terbaru
- RAM: Minimum 4 GB
- Storage: HDD/SSD minimal 256 GB

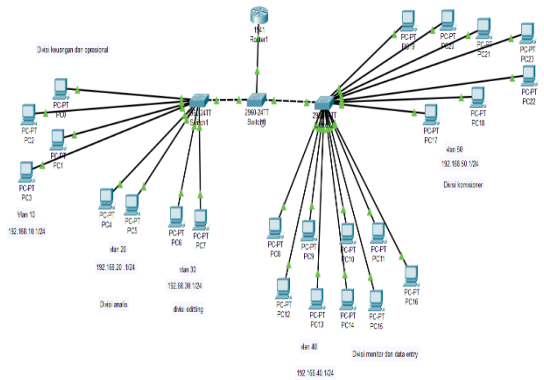
2.2. Software (Perangkat Lunak), yang digunakan sebagai berikut:

2.2.1. Microsoft Windows 11

2.2.2. Cisco Packet Tracer

2.2.3. Aplikasi pendukung lain seperti: command prompt, winscp, dan putty.

3. HASIL DAN PEMBAHASAN



Gambar 1. Topologi Jaringan

Pada gambar 1 di atas dalam struktur jaringan yang diterapkan, Switch 1 berperan sebagai core switch atau server switch, yang menjadi pusat konsolidasi seluruh lalu lintas data jaringan dari berbagai divisi. Switch ini terhubung langsung ke router sebagai perangkat Layer 3 yang menangani proses routing antar

VLAN. Core switch ini menangani VLAN 10 (Keuangan), VLAN 20 (Analis), dan VLAN 30 (Editing), sekaligus menjadi penghubung utama bagi Switch 2 dan Switch 3 melalui koneksi trunk. Fungsi trunking ini memungkinkan pengiriman berbagai VLAN melalui satu jalur fisik tanpa kehilangan segmentasi antar divisi. Sementara itu, Switch 2 dan Switch 3 berperan sebagai access switch atau client switch, masing-masing melayani VLAN 40 (Monitor & Data Entry) dan VLAN 50 (Komisioner). Kedua switch ini dikonfigurasi dengan port access untuk setiap divisi, dan mengirimkan data ke Switch 1 melalui trunk port, tanpa komunikasi langsung ke router.

Dengan diterapkannya *VLAN trunking* antara Switch 1 ke router, serta dari Switch 1 ke Switch 2 dan Switch 3, jaringan ini mampu mengisolasi lalu lintas antar VLAN. Isolasi ini memastikan bahwa komunikasi antar divisi hanya dapat terjadi melalui proses routing yang dikendalikan oleh router, sehingga meningkatkan keamanan data, mengurangi collision domain, dan mempercepat kinerja jaringan. Dalam arsitektur ini, jaringan dibangun dengan pendekatan hierarchical switching yang terbagi menjadi dua lapisan: core layer yang diwakili oleh Switch 1, dan access layer yang diwakili oleh Switch 2 dan Switch 3. Struktur ini tidak hanya memberikan efisiensi dalam pengelolaan lalu lintas data, tetapi juga memungkinkan pengembangan jaringan di masa mendatang secara lebih mudah dan terukur

3.1. Konfigurasi

Berikut ini adalah konfigurasi berdasarkan topologi jaringan vlan diatas:

1. Konfigurasi Router Cisco 1941 menggunakan metode (Router-on-a-Stick)

```
Router>enable
Router#conf t
Router(config)#interface GigabitEthernet0/0
Router(config-if)#no sh
Router(config-if)#ex
Router(config)#interface GigabitEthernet0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config)#interface GigabitEthernet0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config)#interface GigabitEthernet0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config)#interface GigabitEthernet0/0.40
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.40.1 255.255.255.0
Router(config)#interface GigabitEthernet0/0.50
Router(config-subif)#encapsulation dot1Q 50
Router(config-subif)#ip address 192.168.50.1 255.255.255.0
```

2. Konfigurasi Switch Cisco 2960-24TT (1 server)

```
Switch(config)#vlan 10
Switch(config-vlan)#name keuangan&operasional
Switch(config)#vlan 20
Switch(config-vlan)#name analis
Switch(config)#vlan 30
Switch(config-vlan)#name editing
Switch(config)#vlan 40
Switch(config-vlan)#name monitor&dataentry
Switch(config)#vlan 50
Switch(config-vlan)#name komisioner
Switch(config)#interface range fa0/1-2
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk allowed vlan 1,10,20,30,40,50
Switch(config-if-range)#vtp domain kpid.net
Switch(config)#vtp password xxxxxxxx
Switch(config)#vtp mode server
```

3.Konfigurasi Switch Cisco 2960-24TT (2 client)

```
Switch(config)#interface fa0/2
Switch(config-if)#switchport mode access
```

Switch(config-if)#switchport access vlan 10
Switch(config)#interface fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config)#interface fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config)#interface fa0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config)#interface fa0/6
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config)#interface fa0/7
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config)#interface fa0/8
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config)#interface fa0/9
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30

4.Konfigurasi Switch Cisco 2960-24TT (3 client)

Switch(config)#interface fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allow vlan 1,10,20,30,40,50
Switch(config)#interface fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 40
Switch(config)#interface fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 40
Switch(config)#interface fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 40
Switch(config)#interface fa0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 40
Switch(config)#interface fa0/6
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 40
Switch(config)#interface fa0/7
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 40
Switch(config)#interface fa0/8
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 40
Switch(config)#interface fa0/9
Switch(config-if)#interface fa0/9
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 40
Switch(config)#interface fa0/10
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 40
Switch(config)#interface fa0/18
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 40
Switch(config)#interface fa0/19
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 40
Switch(config)#interface fa0/20
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 40
Switch(config)#interface fa0/11
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 50
Switch(config)#interface fa0/12
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 50
Switch(config)#interface fa0/13
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 50
Switch(config)#interface fa0/14
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 50
Switch(config)#interface fa0/15
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 50
Switch(config)#interface fa0/16
Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 50
Switch(config)#interface fa0/17
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 50

3.2. Pembagian IP

Tabel 1. Divisi Keuangan dan Oprasional (VLAN 10)

PC	IP Address	Subnet Mask	Gateway
0	192.168.10.1	255.255.255.0	192.168.10.1
1	192.168.10.2		
2	192.168.10.3		
3	192.168.10.4		

Tabel 2. Divisi Analis(VLAN 20)

PC	IP Address	Subnet Mask	Gateway
4	192.168.20.1	255.255.255.0	192.168.20.1
5	192.168.20.2		

Tabel 3. Divisi Editing(VLAN 30)

PC	IP Address	Subnet Mask	Gateway
6	192.168.30.1	255.255.255.0	192.168.30.1
7	192.168.30.2		

Tabel 4. Divisi monitor isi siaran dan Data Entry (VLAN 40)

PC	IP Address	Subnet Mask	Gateway
8	192.168.40.1	255.255.255.0	192.168.40.1
9	192.168.40.2		
10	192.168.40.3		
11	192.168.40.4		
12	192.168.40.5		
13	192.168.40.6		
14	192.168.40.7		
15	192.168.40.8		
16	192.168.40.9		
24	192.168.40.10		
25	192.168.40.11		

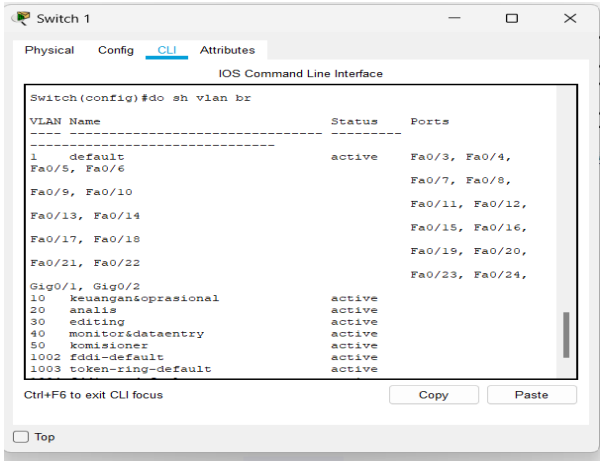
Tabel 5. Divisi komisioner(VLAN 50)

PC	IP Address	Subnet Mask	Gateway
9	192.168.50.1	255.255.255.0	192.168.50.1
0	192.168.50.2		
1	192.168.50.3		
3	192.168.50.4		
7	192.168.50.5		
8	192.168.50.6		
2	192.168.50.7		

3.3. Pengujian Jaringan dan Keamanan

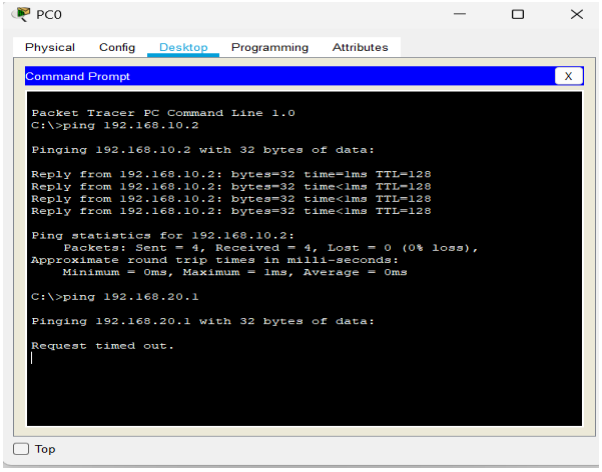
Pengujian kecepatan jaringan dilakukan untuk mengevaluasi seberapa cepat data dapat ditransfer antar perangkat dalam jaringan yang telah dibangun. Dalam simulasi menggunakan Cisco Packet Tracer, pengujian dilakukan dengan cara mengirimkan paket data dari satu perangkat ke perangkat lain menggunakan perintah ping maupun fitur Add Simple PDU. Mode simulasi digunakan untuk memvisualisasikan alur pergerakan paket, serta memperlihatkan waktu tempuh logis dari pengiriman data tersebut. Meskipun tidak menampilkan kecepatan transfer data secara real-time dalam satuan Mbps, simulasi ini berguna untuk mengamati efisiensi jalur komunikasi, deteksi kemungkinan bottleneck, serta keberhasilan konektivitas antar perangkat. Hasil pengujian menunjukkan bahwa data dapat dikirimkan dengan lancar dan waktu tempuh yang singkat, menandakan bahwa konfigurasi jaringan telah berjalan dengan baik dan tidak terdapat hambatan komunikasi antar node jaringan.

3.4. Hasil dan Analisis



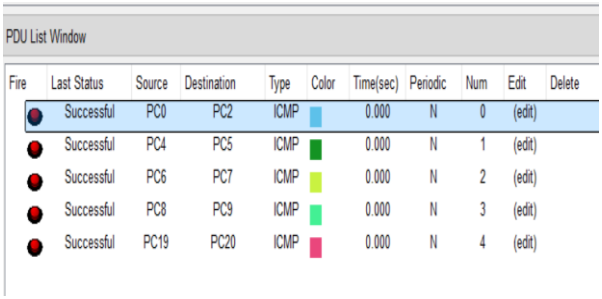
Gambar 2. Mengecek Status VLAN

Berdasarkan pada gambar 2, VLAN 10, 20, 30, 40, dan 50 semuanya dalam kondisi aktif dan siap digunakan pada switch. Setiap VLAN telah memiliki nama yang representatif sesuai fungsinya, seperti VLAN 10 untuk keuangan dan operasional, VLAN 20 untuk analis, VLAN 30 untuk editing, VLAN 40 untuk monitor dan data entry, serta VLAN 50 untuk komisioner. Status aktif ini menandakan bahwa VLAN tersebut telah dikonfigurasi dengan benar dan dapat digunakan untuk memisahkan traffic jaringan sesuai kebutuhan.



Gambar 3. Tes Ping

Hasil ping yang menunjukkan suksesnya komunikasi dari IP 192.168.10.2 mengindikasikan bahwa VLAN trunk yang membawa VLAN 10 berfungsi dengan baik, sehingga perangkat yang berada dalam VLAN tersebut dapat saling terhubung dan bertukar data tanpa hambatan. Namun, kegagalan ping ke IP 192.168.20.1 dengan pesan "Request timed out" menandakan adanya masalah pada VLAN 20, yang mungkin disebabkan oleh konfigurasi trunk yang tidak mengizinkan VLAN 20 . Begitu juga dengan PC lainya yang berada dalam vlan yang sama akan bisa berkomunikasi sedangkan yang tidak berada di vlan yang sama tidak akan bisa berkomunikasi



Gambar 4. Pengujian lalu lintas di VLAN yang sama

Berdasarkan hasil pengujian pada simulasi Cisco Packet Tracer yang ditampilkan dalam jendela PDU List Window, dapat disimpulkan bahwa komunikasi antar perangkat dalam jaringan VLAN yang sama berjalan dengan sukses. Hal ini ditunjukkan oleh status Successful pada setiap paket ICMP yang dikirim dari PC sumber ke PC tujuan. Beberapa pasangan perangkat yang diuji, seperti PC0 ke PC2, PC4 ke PC5, dan PC19 ke PC20, berhasil saling berkomunikasi tanpa hambatan, yang mengindikasikan bahwa mereka berada dalam VLAN yang sama dan *VLAN trunking* telah dikonfigurasi dengan benar. Seluruh proses pengiriman paket tercatat memiliki waktu tempuh 0.000 detik, menunjukkan bahwa tidak terjadi delay ataupun gangguan dalam aliran data. Keberhasilan pengujian ini menunjukkan bahwa segmentasi jaringan melalui VLAN telah berhasil diimplementasikan dan trunking antar switch atau perangkat jaringan bekerja sesuai fungsinya, memungkinkan lalu lintas data antar VLAN yang sama melewati trunk port tanpa gangguan. Dengan demikian, jaringan yang dibangun telah menunjukkan performa yang baik dalam hal konektivitas dan segmentasi logis.

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC0	PC4	ICMP		0.000	N	0	(edit)	
	Failed	PC5	PC6	ICMP		0.000	N	1	(edit)	
	Failed	PC7	PC8	ICMP		0.000	N	2	(edit)	
	Failed	PC8	PC17	ICMP		0.000	N	3	(edit)	

Gambar 5. Pengujian lalu lintas di VLAN berbeda

Berdasarkan hasil pengujian pada simulasi yang ditampilkan dalam gambar PDU List Window, terlihat bahwa seluruh pengiriman paket ICMP antar perangkat mengalami kegagalan, yang ditunjukkan dengan status "Failed" pada setiap percobaan komunikasi. Beberapa pasangan perangkat seperti PC0 ke PC4, PC5 ke PC6, dan PC7 ke PC8 tidak dapat saling terhubung. Kegagalan komunikasi ini menunjukkan bahwa segmentasi jaringan melalui VLAN telah berhasil diterapkan. Hal ini disebabkan oleh konfigurasi VLAN yang membatasi komunikasi antar perangkat yang berada di VLAN yang berbeda. Dengan tidak adanya komunikasi lintas VLAN, maka setiap perangkat hanya dapat berkomunikasi dengan perangkat lain yang berada dalam VLAN yang sama. Oleh karena itu, hasil pengujian ini mengindikasikan bahwa mekanisme segmentasi jaringan bekerja sebagaimana mestinya, yaitu memisahkan lalu lintas antar VLAN untuk meningkatkan keamanan dan efisiensi jaringan.

3.4.1. Uji Reliabilitas

Uji *Reliabilitas* (*Stress Ping*) yang dilakukan dengan mengirimkan 200 paket ke alamat 192.168.20.1 menunjukkan koneksi jaringan yang sangat stabil dan memiliki performa tinggi. Hasil *output* didominasi oleh pesan "*Reply from 192.168.20.1*" yang konsisten, tanpa terlihat adanya kegagalan atau packet loss ("*Request timed out*"), yang mengindikasikan bahwa jaringan berhasil menangani beban pengiriman paket ICMP secara terus-menerus. Selain *stabilitas*, kecepatan respon *(latency*) yang dicapai sangat impresif, dengan sebagian besar waktu respon berada pada nilai kurang dari 1 milidetik (<1ms) hingga 2 milidetik (2ms), dan hanya sesekali

```
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.1 -n 200

Pinging 192.168.20.1 with 32 bytes of data:

Reply from 192.168.20.1: bytes=32 time=2ms TTL=128
Reply from 192.168.20.1: bytes=32 time<1ms TTL=128
Reply from 192.168.20.1: bytes=32 time<1ms TTL=128
Reply from 192.168.20.1: bytes=32 time<1ms TTL=128
Reply from 192.168.20.1: bytes=32 time<1ms TTL=128
Reply from 192.168.20.1: bytes=32 time<1ms TTL=128
Reply from 192.168.20.1: bytes=32 time=3ms TTL=128
Reply from 192.168.20.1: bytes=32 time=2ms TTL=128
Reply from 192.168.20.1: bytes=32 time<1ms TTL=128
Reply from 192.168.20.1: bytes=32 time<1ms TTL=128
Reply from 192.168.20.1: bytes=32 time=2ms TTL=128
Reply from 192.168.20.1: bytes=32 time=3ms TTL=128
Reply from 192.168.20.1: bytes=32 time<1ms TTL=128
Reply from 192.168.20.1: bytes=32 time=2ms TTL=128
Reply from 192.168.20.1: bytes=32 time<1ms TTL=128
Reply from 192.168.20.1: bytes=32 time<1ms TTL=128
Reply from 192.168.20.1: bytes=32 time=1ms TTL=128
Reply from 192.168.20.1: bytes=32 time<1ms TTL=128
Reply from 192.168.20.1: bytes=32 time<1ms TTL=128
Reply from 192.168.20.1: bytes=32 time=3ms TTL=128
```

mencapai 3ms. *Latency* yang sangat rendah ini membuktikan bahwa jalur komunikasi (termasuk perangkat *inter-networking* yang mungkin terlibat) berfungsi dengan efisiensi optimal. Nilai TTL=128 yang konsisten juga menegaskan bahwa topologi jaringan stabil dan paket selalu mengikuti jalur yang sama. Secara keseluruhan, pengujian ini memvalidasi bahwa koneksi ke perangkat tujuan 192.168.20.1 adalah *reliabel*, cepat, dan mampu beroperasi secara efektif di bawah beban *stress ping.*

Gambar 6. Uji *Reliabilitas*

3.4.2. Perbandingan

Hasil perbandingan antara Kondisi Awal (192.168.199.84) dan Kondisi Akhir (192.168.20.1) menunjukkan peningkatan kinerja jaringan yang sangat signifikan setelah dilakukan konfigurasi. Pada aspek Reliabilitas (*Packet Loss*), kedua kondisi menunjukkan performa yang sempurna, di mana semua paket yang terlihat berhasil diterima tanpa adanya *loss* atau kehilangan paket. Namun, perbedaan utama dan yang paling krusial terletak pada Kinerja jaringan, yang diukur melalui *Latensi* atau waktu tempuh paket. Sebelum konfigurasi, jaringan berada dalam kondisi Tidak Stabil dan cenderung Lambat, ditandai dengan Latensi Terendah 9 ms dan lonjakan Latensi Tertinggi yang ekstrem mencapai 202 ms. Rentang waktu yang lebar ini menghasilkan *Stabilitas* (*Jitter/Fluktuasi*) yang dinilai Tinggi/Buruk, menunjukkan adanya hambatan, kemacetan, atau beban kerja yang tinggi pada host tujuan selama stress test berlangsung. Sebaliknya, setelah konfigurasi, kondisi jaringan berubah menjadi Sangat Stabil dan Sangat Cepat. *Latensi* Terendah turun drastis menjadi <1 ms, dan *Latensi* Tertinggi hanya mencapai 3 ms. Perubahan ini menghasilkan Stabilitas yang

Sangat Rendah/Sempurna, membuktikan bahwa konfigurasi jaringan yang diterapkan berhasil mengoptimalkan jalur komunikasi, menghilangkan *bottleneck*, dan secara efektif menekan *jitter* (fluktuasi waktu) ke tingkat yang minimal.

Tabel 6. Perbandingan sebelum dan sesudah penerapan Trunk

Kriteria	Kondisi Awal	Kondisi Akhir
Lingkungan	Command Prompt Windows/DOS	Packet Tracer (PC Command Line 1.0)
Reliabilitas (Packet Loss)	Sempurna (0% loss pada paket yang terlihat)	Sempurna (0% loss pada paket yang terlihat
Latensi Terendah (Minimum Time)	9 ms	<1 ms (Sangat Cepat)
Latensi Tertinggi (Maximum Time)	202 ms	3 ms (Sangat Cepat)
Stabilitas (Jitter/Fluktuasi)	Tinggi/Buruk (Rentang waktu lebar: 9ms hingga 202ms).	Sangat Rendah/Sempurna (Rentang waktu sangat sempit: <1ms hingga 3ms).
Kesimpulan Kinerja	Tidak Stabil dan cenderung Lambat	Sangat Stabil dan Sangat Cepat

Jika konfigurasi telah diterapkan dan berjalan dengan baik, maka anggota Divisi Analisis tidak akan bisa mendapatkan atau mengakses IP segmen Divisi Editing, dan oleh karena itu tidak dapat mengakses komputer-komputer di divisi tersebut, karena tujuan utama dari VLAN (*Virtual Local Area Network*) adalah untuk menciptakan isolasi trafik antar segmen jaringan. Setiap divisi, seperti Analisis dan Editing, ditempatkan pada ID VLAN yang berbeda begitu juga dengan divisi lainnya yang ada dan segmen IP address yang berbeda pula, yang berarti mereka berada dalam domain broadcast logis yang sepenuhnya terpisah di Layer 2; komputer Divisi Analisis hanya akan menerima broadcast dan IP dari subnet VLAN-nya sendiri. Sementara itu, VLAN Trunking hanya bertugas membawa paket data dari kedua VLAN yang berbeda ini melalui satu kabel fisik antara *switch* (menggunakan *tagging 802.1Q*), tetapi *switch* akan memastikan bahwa paket yang telah di tag dengan ID VLAN Analisis hanya diteruskan ke port yang menjadi anggota VLAN Analisis, sehingga isolasi antar divisi tetap terjaga dan akses ke divisi lain akan terblokir secara otomatis tanpa adanya perangkat *router Layer* 3 yang mengizinkan komunikasi antar-VLAN (*Inter-VLAN Routing*).

4. PENUTUP

4.1. Kesimpulan

Berdasarkan hasil implementasi dan pengujian jaringan menggunakan konsep VLAN dan pengaturan trunking pada topologi yang telah dirancang, dapat disimpulkan bahwa jaringan berhasil dibangun dengan baik dan berfungsi sesuai harapan. Pengujian konektivitas antar perangkat yang berada dalam VLAN yang sama menunjukkan hasil yang sukses, di mana paket data dapat dikirim tanpa kendala, yang membuktikan bahwa *VLAN trunking* telah dikonfigurasi secara tepat. Selain itu, hasil pengujian juga menunjukkan bahwa perangkat dari VLAN yang berbeda tidak dapat saling berkomunikasi tanpa inter-VLAN routing, yang menandakan segmentasi jaringan berhasil meningkatkan keamanan dan efisiensi lalu lintas data. Implementasi ini mendukung kebutuhan jaringan secara fungsional maupun non-fungsional, termasuk kecepatan akses, reliabilitas, dan keamanan. Dengan demikian, sistem jaringan yang dibangun telah memenuhi tujuan penelitian, yaitu menciptakan jaringan yang tersegmentasi, aman, serta mendukung komunikasi internal dengan performa yang baik

4.2. Saran

Berdasarkan hasil penelitian dan implementasi yang telah dilakukan, penulis menyadari bahwa meskipun sistem jaringan dengan teknologi VLAN dan trunking telah terbukti mampu meningkatkan segmentasi, efisiensi, dan keamanan, masih terdapat beberapa hal yang dapat dikembangkan lebih lanjut. Penulis menyarankan agar penelitian selanjutnya dapat mengeksplorasi penerapan inter-VLAN routing secara lebih mendalam, khususnya dengan melibatkan perangkat router atau Layer 3 switch untuk memungkinkan komunikasi terkontrol antar VLAN tanpa mengorbankan keamanan.

5. DAFTAR PUSTAKA

Ainurrachman, R., & Yahya, W. (2017). *Analisis Perbandingan Metode VLAN dan MAC- based dalam Penerapan Segmentasi Jaringan pada Jaringan OpenFlow*. *1*(1), 1–11.

Alfian, T., Sandi, A., Anwar, R. S., & Fauzi, A. (2023). *Analisis Performa Redundancy Link Menggunakan Metode Spanning Tree Protocol dan Per VLAN Spanning Tree*. *5*(1), 47–52.

Amisyah, H. (2025). *Optimasi Jaringan dengan Virtual LAN (VLAN) untuk Meningkatkan Efisiensi Data Transfer*. *5*(2), 90–97.

Dawson, C. (2019). *A – Z of Digital Research Methods*.

Elimanafe, R., Suban Belutowe, Y., Katemba, P., Kupang Jln Perintis Kemerdekaan, U. I., Putih, K., & Kupang Nusa Tenggara Timur, K. (2022). Perancangan Jaringan Virtual Local Area Network (VLAN) untuk Menunjang Transaksi Data antar Jaringan. *Jurnal Teknologi Informasi*, *6*(1), 102–111.

Farizy, S. (2025). *Buku Ajar Jaringan Komputer : Dari Teori Dasar Hingga Jaringan Nirkabel*.

Febrian, A. D., & Darmawan, R. (2022). *Implementasi Jaringan Komputer Berbasis Virtual LAN untuk Layanan Iconnet VIP pada Jaringan MPLS (Multi Protocol Label Switching): Studi Kasus di PT Indonesia Comnets*. *2*(3), 466–480.

Handono, F. W., Darono, H. E., Nuryadi, N., & Suryanto, A. (2024). *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*. *8*(2), 252–263. https://doi.org/10.52362/jisicom.v8i2.1663

Harun Ar Rasyid1), Satrio Broto2), W. A. (2024). *Optimasi Infrastuktur Jaringan VLAN Trunking Protocol Menggunakan Simulasi Packet Tracer pada PT. RUKUN SEJAHTRA TEKNIK*. *04*.

Haryoyudhanto, H. D., Fitri, I., Aningsih, A., Studi, P., Informatika, T., & Nasional, U. (2022). *Implementasi Encapsulation Jaringan Redudansi VLAN Menggunakan Metode Hot Standby Router Protocol (HSRP)*. *3*(28), 49–54.

Julandra, B. P., & Mabruri, A. (2022). *Analisis dan Perancangan Jaringan Local Area Network pada LAB Komputer DI SMK NEGERI 5 KOTA SERANG*. *4*(3), 121–134. https://doi.org/10.55642/eatij.v4i0

Noviriandini, A., Bachtiar, D., & Indriyani, L. (2023). *Perancangan Jaringan Virtual Local Area Network Menggunakan Cisco Packet Tracer pada SMK Islam Assa ' adatul Abadiyah*. *5*, 255–260.

Nurbahri, R. (2021). *Perancangan dan Implementasi Virtual Local Area Network (Vlan) untuk Optimalisasi Bandwidth Jaringan*. *1*(1), 13–18.

Nurfaishal, M. D., & Akbar, Y. (2024). *Analisis Efektivitas Keamanan Jaringan Layer 2 : Port Security , VLAN Hopping , DHCP Snooping Abstrak*. *5*(3), 3278–3290.

Octavian, A., & Purnama, G. (2024). *Perancangan Jaringan Redudancy Menggunakan Konsep Etherchannel Dan HSRP dengan InterVlan Routing Pada*

PLN UID JAKARTA RAYA. *12*(2).

Pirzi Kurniawan, K. S. (2022). *Pengembangan VLAN dengan VLAN Trungking Protocol (VTP) Mode Menggunakan Switch Cisco Di BANK SYARIAH INDONESIA*. *1*(08), 1226–1233.

Prasetyo Dwi Hidayat Paputungan , Pitrasacha Adytia, dan M. F. (2024). *Implementasi Keamanan Jaringan LAN Berbasis VLAN Studi Kasus STMIK WIDYA CIPTA DHARMA*. *25*.

Purbo, O. W. (2020). *Analysis and Implementation Of Virtual Local Area Network (VLAN) Design Using Pox Controller*. *09*(01), 106–115.

Putri Intan Octavia Br Sipayung1, Viviana Purba2*, A. (2024). *Analisis, Perancangan, dan Simulasi Jaringan VLAN Menggunakan Metode PPDIOO (Studi Kasus: SMAS Santo Yusup Surabaya)*. *14*(1), 110–118.

Rahman, T., Zaini, T. R., & Chrisnawati, G. (2020a). Perancangan Jaringan Virtual Local Area Network (Vlan) & Dhcp pada Pt.Navicom Indonesia Bekasi. *JIKA (Jurnal Informatika)*, *4*(1), 36. https://doi.org/10.31000/jika.v4i1.2366

Rahman, T., Zaini, T. R., & Chrisnawati, G. (2020b). Perancangan Jaringan Virtual Local Area Network (Vlan) & Dhcp Pada Pt.Navicom Indonesia Bekasi. *JIKA (Jurnal Informatika)*, *4*(1), 36. https://doi.org/10.31000/jika.v4i1.2366

Rudy Salam, J. T. (2022). *Perancangan dan Implementasi VLAN dengan VLAN Trungking Protocol (VTP) di PT. CITRA SOLUSI PRATAMA*. *8*(2), 91–105.

Sakti, M. G., Nugroho, K., Gusti, J., & Ginting, A. (2020). *Analisis Pengaruh Penggunaan VTP Pruning pada Jaringan VLAN*. *8275*, 48–57.

Setiawan1, B., Purwani2, D., Laily3, D. Y., Fadhilah, F., & Ali4. (2022). *Kantor Desa SAMBIREJO TIMUR Menggunakan Cisco Packet Tracer*. 1–7.

Sholid, G., Kom, M., Kom, M., Sari, R. S., & Kom, M. (2025). *Implementasi Jaringan Virtual Local Area Network Dengan Cisco Packet Tracer Untuk Manajemen Traffic Jaringan Kampus*. *2*, 29–38. https://doi.org/10.70308/grata.v2i1.71

Sopian, A., Khoiriyah, K., & Gonti, I. D. P. (2022). Perancangan Jaringan Virtual Lan Menggunakan Metode Protokol Peer-Vlan Spanning Tree. *Jeis: Jurnal Elektro Dan Informatika Swadharma*, *2*(1), 28–35. https://doi.org/10.56486/jeis.vol2no1.157

Stefan, D., Kurniawan, A., Cahya, S. D., Laily, I. N., & Adryan, M. (2024). *Network Automation VLAN pada Switch Menggunakan Python*. *3*(1), 165–173.

Sujana, J. (2022). *Implementasi Virtual Local Area Network dengan Basis Inter-Vlan Routing Menggunakan Mikrotik*. 47–61.

Sunarsan Sitohang1), H. P. (2025). *Analisis Keamanan dan Kinerja Jaringan pada Implementasi VLAN Sebagai Upaya Segmentasi Trafik Menggunakan Cisco Packet Tracer*. 264–270.

Wibowo, A. (2024). *Teori & Pratik Jaringan Komputer*.

Widyastuti, I., & Hendrian, Y. (2022). Pemanfaatan VLAN Untuk Meningkatkan Kinerja Jaringan Komputer BKPP Kabupaten Bogor. *Computer Science (CO-SCIENCE)*, *2*(1), 10–18. https://doi.org/10.31294/coscience.v2i1.894