Implementasi dan Konfigurasi VLAN Menggunakan Cisco *Packet Tracer* untuk Optimalisasi Jaringan

VLAN Implementation and Configuration Using Cisco *Packet Tracer* for Network Optimization

Abelia Naja Salma Kalisa[1*], Endah Setyowati[2]
[1,2]Universitas Pendidikan Indonesia
[1,2]Jl. Dr. Setiabudi No.229, Isola, Kec. Sukasari, Kota Bandung, Jawa Barat 40154
abelianaja@upi.edu[1*], endahsetyowati@upi.edu[2]

Abstrak – *Penelitian ini bertujuan untuk mengimplementasikan dan mengonfigurasi Virtual Local Area Network (VLAN) dengan Cisco Packet Tracer guna mengoptimalkan jaringan. Latar belakang permasalahan penelitian ini didasari oleh kebutuhan akan jaringan yang efisien dan aman dalam lingkungan lokal seperti kampus atau kantor. Metode penelitian yang digunakan adalah metode eksperimental dengan memanfaatkan perangkat lunak simulasi Cisco Packet Tracer versi 8.2.1. Simulasi dilakukan pada dua skenario konfigurasi VLAN, yaitu tanpa trunking dan dengan trunking. Hasil pengujian menunjukkan bahwa rata-rata latency berada pada kisaran 5,2–7,1 ms, throughput stabil di atas 940–980 kbps, dan packet loss tercatat 0% pada seluruh skenario. Dibandingkan konfigurasi dasar tanpa trunking, penggunaan trunking menyebabkan kenaikan latency sekitar 30–36% (dari 5,2 ms menjadi 6,8–7,1 ms) serta sedikit penurunan throughput sebesar 3–4% (dari 980 kbps menjadi 940–950 kbps) akibat overhead tagging IEEE 802.1Q, namun tetap menjaga performa jaringan dalam kategori baik. Selain itu, isolasi VLAN terbukti mampu menurunkan broadcast traffic dan meningkatkan keamanan dengan membatasi akses antar perangkat pada VLAN berbeda. Dengan demikian, konfigurasi VLAN dapat diimplementasikan secara efektif untuk optimalisasi jaringan lokal dari sisi efisiensi, kinerja, dan keamanan.*

Kata Kunci*: VLAN, Cisco Packet Tracer, jaringan, keamanan, efisiensi, trunking.*

Abstract – *This study aims to implement and configure a Virtual Local Area Network (VLAN) using Cisco Packet Tracer in order to optimize network performance. The research background is based on the need for an efficient and secure network within local environments such as campuses or offices. The research method applied is an experimental approach utilizing Cisco Packet Tracer version 8.2.1. The simulation was conducted under two VLAN configuration scenarios: without trunking and with trunking. The test results indicate that the average latency ranged from 5.2 to 7.1 ms, throughput remained stable at 940–980 kbps, and packet loss was recorded at 0% in all scenarios. Compared to the basic configuration without trunking, the use of trunking resulted in an increase in latency of approximately 30–36% (from 5.2 ms to 6.8–7.1 ms) and a slight decrease in throughput of about 3–4% (from 980 kbps to 940–950 kbps) due to IEEE 802.1Q tagging overhead, while still maintaining overall network performance within a good category. Furthermore, VLAN isolation was proven to reduce broadcast traffic and enhance security by restricting access between devices in different VLANs. Therefore, VLAN configuration can be effectively implemented to optimize local networks in terms of efficiency, performance, and security.*

Keywords*: VLAN, Cisco Packet Tracer, network, security, efficiency, trunking.*

1. Pendahuluan

Di era digital saat ini, teknologi dan informasi berkembang dengan pesat, mendorong perubahan signifikan dalam berbagai aspek kehidupan, termasuk dalam jaringan komputer yang memfasilitasi pengelolaan dan penyimpanan informasi. Cisco Packet Tracer adalah salah satu aplikasi simulasi jaringan yang sangat relevan dalam konteks ini karena memungkinkan pengembangan keterampilan dasar hingga lanjutan dalam perancangan dan manajemen jaringan komputer. Cisco Packet Tracer memungkinkan pengguna untuk membuat, memvisualisasikan, dan menguji konfigurasi jaringan tanpa memerlukan perangkat keras fisik [1]. Cisco Packet Tracer membantu dalam pemahaman konsep dasar jaringan seperti *subnetting*, *routing*, dan VLAN yang relevan dengan teknologi saat ini. Karena semua simulasi dilakukan secara virtual, tidak perlu membeli perangkat keras jaringan yang mahal, sehingga membantu lembaga pendidikan dan pelajar untuk berlatih tanpa investasi besar. Namun terdapat pula kekurangan dari *tools* ini yakni Cisco Packet Tracer tidak memiliki semua fitur yang dimiliki perangkat jaringan Cisco yang sebenarnya [2], [3]. Selain itu Cisco Packet Tracer tidak ideal untuk simulasi jaringan besar atau kompleks. Ketika terlalu banyak perangkat ditambahkan, performa aplikasi bisa menurun, menyebabkan lag atau bahkan *crash*, sehingga kurang ideal untuk simulasi topologi jaringan dengan skala yang besar [4]. Oleh karena itu dilakukan penelitian ini untuk menguji optimalisasi jaringan pada aplikasi Cisco Packet Tracer.

Salah satu bentuk jaringan yang sering digunakan dalam lingkup lokal adalah *Local Area Network* (LAN). Jaringan LAN memiliki peran penting sebagai infrastruktur dasar untuk menghubungkan berbagai perangkat dalam area terbatas, seperti dalam kantor, sekolah, atau kampus. LAN memungkinkan perangkat-perangkat tersebut untuk saling berkomunikasi dan bertukar data melalui jaringan yang dikelola secara lokal. Seiring dengan meningkatnya kebutuhan jaringan yang efisien dan aman, muncul teknologi *Virtual Local Area Network* (VLAN) yang memperluas kemampuan LAN tradisional. VLAN merupakan konsep jaringan yang memungkinkan pembagian jaringan LAN fisik menjadi beberapa jaringan logis terpisah, walaupun menggunakan perangkat fisik yang sama seperti *switch*. Ketika dua atau lebih jaringan LAN yang berbeda saling terkoneksi menggunakan satu switch yang sama, maka jaringan tersebut dapat dikategorikan sebagai VLAN [5]. Konfigurasi VLAN ini dirancang untuk menghubungkan perangkat di lokasi yang sama, tetapi secara logis memisahkan lalu lintas data untuk tujuan pengaturan, keamanan, dan efisiensi.

Menurut penelitian yang dilakukan oleh Yoga dan Raharja [3] berpendapat bahwa VLAN dapat membantu mengatasi masalah broadcast domain dalam LAN tradisional dengan membatasi lalu lintas siaran antar perangkat di dalam satu VLAN. VLAN membagi satu switch fisik menjadi beberapa jaringan logis yang terisolasi [6], [7]. Perangkat yang berada dalam VLAN yang sama dapat berkomunikasi satu sama lain seolah-olah berada dalam jaringan fisik yang sama, meskipun mereka berada di subnet yang berbeda. VLAN juga memungkinkan konfigurasi khusus pada setiap ID VLAN untuk mengontrol akses antar perangkat, yang meningkatkan keamanan jaringan secara keseluruhan.

Dalam jaringan konvensional, *router* bertanggung jawab untuk menghentikan lalu lintas siaran (*broadcast traffic*) antar jaringan yang berbeda. Namun, di dalam VLAN, *switch* dapat meneruskan lalu lintas secara otomatis hanya ke *port* yang memiliki ID VLAN yang sama. Dengan kemampuan untuk menangani banyak LAN berbeda melalui VLAN, switch dapat mengarahkan lalu lintas antar perangkat yang termasuk dalam satu grup VLAN *yang* sama, sekaligus mencegah komunikasi dengan perangkat di grup VLAN yang berbeda. Hal ini mengurangi broadcast domain dan meningkatkan efisiensi jaringan [8]. Implementasi VLAN memberikan berbagai keuntungan dalam pengelolaan jaringan, terutama pada jaringan yang kompleks dan memiliki banyak perangkat, diantaranya peningkatan keamanan melalui pemisahan jaringan, pengurangan lalu lintas siaran, dan kemudahan dalam manajemen jaringan. Dalam

ISSN (e): 2540-9123
ISSN (p): 2502-1982

laporan ini, penulis akan membahas implementasi VLAN pada Cisco Packet Tracer, di mana percobaan dilakukan untuk menguji konfigurasi dan kinerja jaringan VLAN pada skenario *multiswitch*. Hasil dari penelitian ini diharapkan dapat menunjukkan manfaat VLAN dalam mengoptimalkan jaringan, serta memberikan pemahaman mengenai konfigurasi VLAN yang efektif untuk meningkatkan keamanan dan kinerja jaringan di lingkungan lokal. Penelitian ini juga mencakup penggunaan teknik *trunking*, yaitu metode untuk menghubungkan beberapa *switch* yang mendukung banyak VLAN sekaligus. *Trunking* pada VLAN yang dilakukan dengan terpisah secara fisik tetap dapat berkomunikasi melalui satu koneksi fisik, yang diperlihatkan pada konfigurasi VLAN 10 dan VLAN 20. Hal ini penting untuk jaringan skala besar yang membutuhkan koneksi antar switch.

Secara eksplisit, penelitian ini mengeksplorasi dua skenario yang berbeda, yaitu konfigurasi VLAN tanpa *trunking* dan dengan *trunking*. Pendekatan ini memberikan gambaran yang lebih komprehensif mengenai penerapan VLAN, baik dalam lingkup satu *switch* maupun antar *switch*. Selain itu, penelitian ini tidak hanya menampilkan konfigurasi dan uji konektivitas, tetapi juga melakukan pengukuran parameter kinerja jaringan berupa *latency*, *throughput*, dan *packet loss*. Dengan metode eksperimental yang bersifat kuantitatif, penelitian ini mampu menghasilkan data objektif yang menunjukkan bahwa VLAN dapat menjaga performa jaringan tetap stabil dengan *latency* rendah, *throughput* di atas 900 kbps, dan *packet loss* minimal. Temuan ini memperkaya literatur yang ada dengan bukti empiris bahwa meskipun trunking menimbulkan sedikit kenaikan *latency* akibat *overhead tagging* IEEE 802.1Q, jaringan tetap efisien, aman, dan fleksibel. Dengan demikian, penelitian ini tidak hanya memperkuat teori yang ada, tetapi juga memberikan kontribusi baru dalam bentuk analisis performa VLAN yang lebih detail.

Tujuan dari penelitian ini mencakup pemahaman bagaimana VLAN dapat digunakan untuk meningkatkan keamanan dan efisiensi jaringan dengan membagi domain siaran (*broadcast domain*), serta menghubungkan perangkat-perangkat di jaringan yang berbeda namun tetap berada dalam satu jaringan fisik, sesuai kebutuhan skenario tertentu.

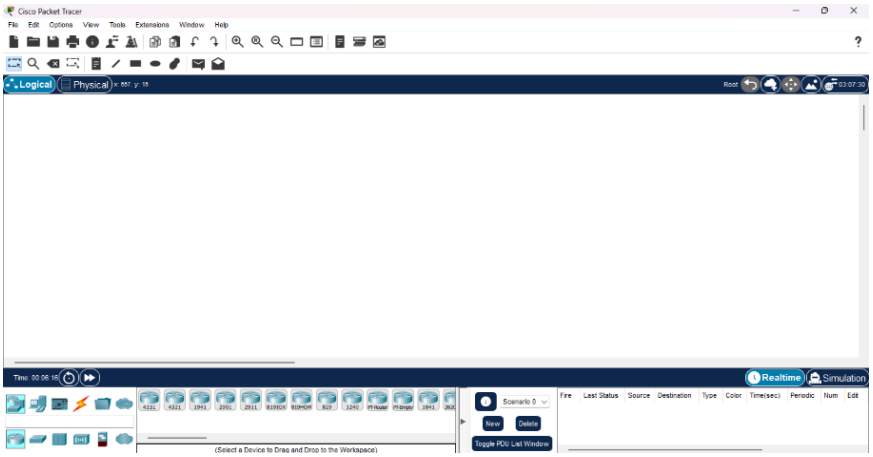
2. Metode Penelitian

Penelitian ini menggunakan metode eksperimental yang dimana umumnya digunakan untuk menguji atau mensimulasikan suatu lalu lintas jaringan. Tujuan utama dari metodologi ini untuk menguji seberapa efektif konfigurasi VLAN dalam meningkatkan kinerja dan keamanan jaringan dan mengurangi *broadcast domain* pada jaringan lokal. Cisco Packet Tracer 8.2.1 digunakan sebagai tools atau simulasi utama. Selain itu laptop yang kompatibel pun perlu disiapkan saat menjalankan simulasi [12]. Pengumpulan data dilakukan dengan melibatkan kajian literatur terkait konsep dasar LAN, VLAN, dan VLAN *trunking*. Selan itu penelitian ini menggunakan metode kualitatif yang bersumber dari literatur meliputi penelitian terdahulu, buku, jurnal ilmiah, dan website resmi dari Cisco Packet Tracer (https://www.netacad.com/dashboard).

Cisco Packet Tracer adalah sebuah perangkat lunak simulasi jaringan yang dikembangkan oleh *Cisco Systems*, *tools* ini dirancang untuk mahasiswa, profesional jaringan, dan teknisi dalam dunia networking. Aplikasi ini memungkinkan pengguna untuk merancang, mensimulasikan, dan mengeksplorasi topologi jaringan kompleks tanpa risiko kerusakan perangkat nyata [12]. Pengambilan data simulasi Cisco Packet Tracer dimulai pada tanggal 20-21 Oktober 2024. Dalam Gambar 1. merupakan tampilan awal ketika membuka aplikasi Cisco Packet Tracer yang didalamnya berisi menu-menu seperti *File*, *Edit*, *Options*, *View*, *Tools*, *Extensions*, *Window*, dan *Help* untuk mengakses berbagai fungsi dalam Packet Tracer.

Kemudian seperti yang terdapat dalam Gambar 2. terdapat ikon-ikon untuk beragam perangkat jaringan seperti *router*, *switch*, *PC*, *server*, dan lain-lain yang dapat digunakan untuk membangun topologi jaringan. Area Panel tengah merupakan area utama tempat pengguna dapat merancang dan mensimulasikan topologi jaringan dengan menyusun perangkat-perangkat yang

tersedia di toolbar bawah. Kemudian Panel di sebelah kiri, menampilkan dua mode utama, yaitu "*Logical*" dan "*Physical*" yang memungkinkan pengguna beralih antara tampilan logis dan fisik dari topologi jaringan. Sedangkan panel sebelah kanan berisi informasi dan kontrol terkait skenario yang sedang disimulasikan, seperti pengaturan waktu, status, sumber, tujuan, jenis, dan warna paket data. Terakhir yakni adanya *toolbar* waktu untuk menampilkan waktu saat simulasi berjalan dan memungkinkan pengguna untuk mengontrol laju simulasi (*realtime* atau *step-by-step*).

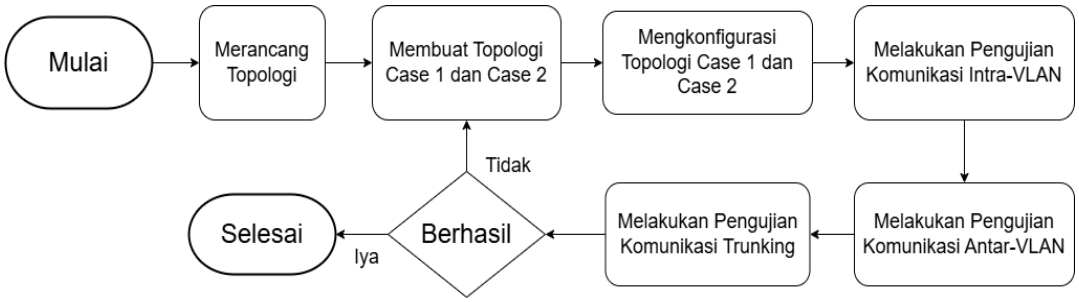


Gambar 1. Tampilan awal cisco packet tracer.

Gambar 2. Komponen perangkat jaringan.

Pada Gambar 3. merupakan diagram alir yang digunakan untuk memudahkan penelitian. Terdapat beberapa langkah yang perlu dilakukan yakni diawali dengan merancang dua topologi. Topologi Case 1 menggunakan 1 perangkat *switch* yang terdiri atas 3 VLAN yaitu VLAN 10 (SISTEL) berisi 4 *host*, VLAN 20 (PGSD) berisi 5 *host*, dan VLAN 30 (PSTI) berisi 6 *host*, sedangkan Topologi Case 2 menggunakan 1 perangkat switch yang terdiri atas 2 VLAN yaitu VLAN 10 (SISTEL) dengan 2 *host* dan VLAN 20 (PGSD) dengan 3 *host*. Hal ini dilakukan guna membuat konfigurasi VLAN dengan dan tanpa *trunking* agar dapat menguji efektivitas masing-masing konfigurasi dalam mengatur lalu lintas jaringan serta keamanan antar perangkat. Setelah itu dilakukan pengujian komunikasi intra-VLAN untuk memastikan perangkat dalam VLAN yang sama dapat saling berkomunikasi. Tahap berikutnya adalah pengujian komunikasi antar-VLAN guna memverifikasi bahwa perangkat pada VLAN berbeda tetap bisa berinteraksi sesuai konfigurasi. Selanjutnya dilakukan pengujian *trunking* untuk mengecek apakah jalur trunk antar perangkat jaringan sudah berfungsi dengan baik. Apabila seluruh pengujian berhasil, proses dianggap selesai, namun jika terdapat kegagalan, maka pengujian akan diulang hingga semua fungsi berjalan sesuai harapan.

ISSN (e): 2540-9123
ISSN (p): 2502-1982

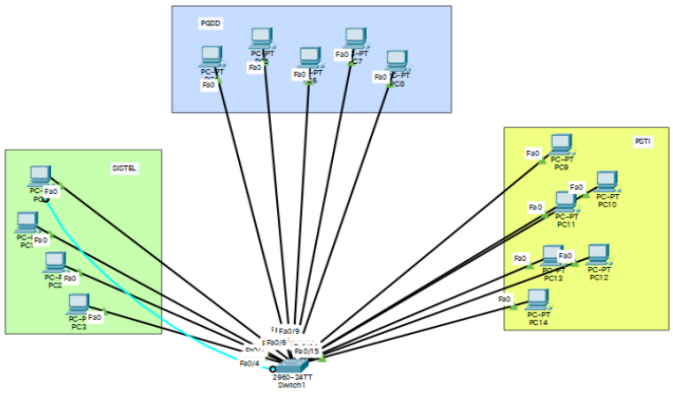


Gambar 3. *Flowchart* desain penelitian.

2.1 Prosedur Eksperimen

Pada topologi case 1, fokus utama adalah melakukan konfigurasi VLAN dasar. Tahapan pertama dimulai dengan perancangan topologi jaringan yang terdiri dari tiga kelompok VLAN. VLAN pertama adalah SISTEL (VLAN 10) yang memiliki 4 *host* dengan penggunaan *subnet* 192.168.10.x. VLAN kedua yaitu PGSD (VLAN 20) terdiri dari 5 *host* menggunakan *subnet* 192.168.20.x. Dan VLAN ketiga adalah PSTI (VLAN 30) yang memiliki 6 *host* dengan *subnet* 192.168.30.x. Untuk desain topologi Setelah perancangan topologi selesai, tahap selanjutnya adalah implementasi yang dimulai dengan melakukan koneksi fisik.

Pada tahap ini, dilakukan penghubungan antara PC dengan *Switch* menggunakan kabel *Straight-Through*. Selain itu, diperlukan juga koneksi khusus antara satu PC dengan *Switch* menggunakan kabel *Console* untuk keperluan konfigurasi. Proses implementasi dilanjutkan dengan konfigurasi VLAN melalui *Command Line Interface* (CLI). Adapun perancangan topologinya sesuai yang terdapat dalam Gambar 4.



Gambar 4. Topologi *case* 1.

Langkah pertama adalah masuk ke mode *enable* dilanjutkan dengan masuk ke *configure terminal*. Setelah itu, dilakukan pembuatan VLAN dengan menentukan *ID* dan nama untuk masing-masing VLAN, serta mengatur *port interfaces* agar sesuai dengan pengelompokan VLAN yang telah dirancang. Selanjutnya dilakukan konfigurasi *IP Address* pada setiap *host* dengan memastikan *subnet mask* sesuai dengan VLAN masing-masing. Tahap terakhir adalah pengujian untuk memastikan konfigurasi VLAN telah berhasil. Pengujian dimulai dengan melakukan verifikasi konfigurasi untuk melihat status dan pengelompokan VLAN. Kemudian dilakukan pengujian konektivitas dengan melakukan PING antar *host* dalam VLAN yang sama untuk memastikan komunikasi berjalan dengan baik.

Terakhir, dilakukan pemeriksaan isolasi antar VLAN yang berbeda untuk memastikan bahwa setiap VLAN telah terisolasi dengan benar sesuai dengan konsep dasar Virtual LAN. Pada bagian ini disajikan hasil simulasi dalam bentuk simulasi dalam Gambar 5. Melalui serangkaian

ISSN (e): 2540-9123
ISSN (p): 2502-1982

tahapan ini, dapat dipastikan bahwa implementasi VLAN dasar telah berhasil dilakukan dengan baik, dimana setiap *host* dapat berkomunikasi dalam VLAN yang sama namun terisolasi dari VLAN yang berbeda. Sedangkan pada bagian ini disajikan hasil simulasi dalam bentuk simulasi dalam Gambar 6.

□

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname kelompok8
kelompok8(config)#vlan 10
kelompok8(config-vlan)#name SISTEL
kelompok8(config-vlan)#exit
kelompok8(config)#vlan 20
kelompok8(config-vlan)#name PGSD
kelompok8(config-vlan)#exit
kelompok8(config)#vlan 30
kelompok8(config-vlan)#name PSTI
kelompok8(config-vlan)#exit
kelompok8(config)#exit
kelompok8#
%SYS-5-CONFIG_I: Configured from console by console

kelompok8#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                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   SISTEL                           active
20   PGSD                             active
30   PSTI                             active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

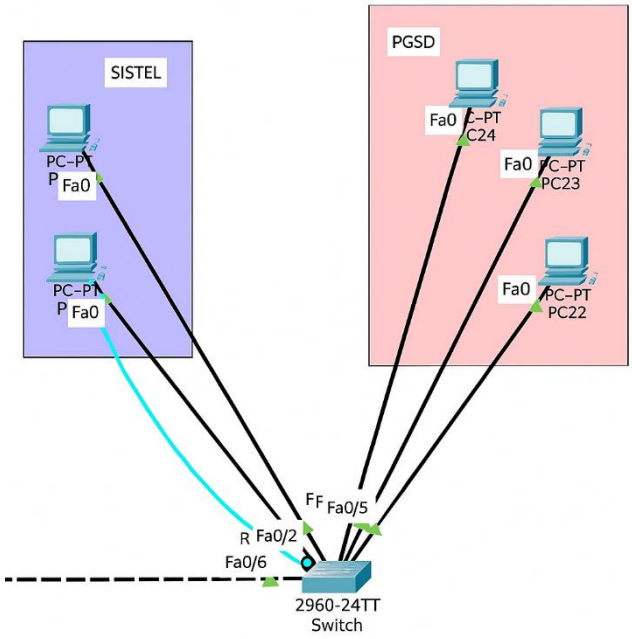
Gambar 5. Konfigurasi *case* 1.

```
kelompok8#show vlan id 10

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
10   SISTEL                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
10   enet  100010     1500  -      -      -        -    -        0      0

kelompok8#show vlan id 20

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
20   PGSD                             active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
20   enet  100020     1500  -      -      -        -    -        0      0

kelompok8#show vlan id 30

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
30   PSTI                             active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
30   enet  100030     1500  -      -      -        -    -        0      0
```

Gambar 6. Konfigurasi pada setiap VLAN.

Pada topologi *case* 2 seperti yang terdapat dalam Gambar 7. mengimplementasikan VLAN *Trunking*, tahapan pertama dimulai dengan perancangan topologi jaringan baru yang akan dihubungkan dengan topologi sebelumnya. Topologi baru ini terdiri dari dua kelompok yaitu VLAN 10 untuk jurusan SISTEL dengan 2 *host* dan VLAN 20 untuk jurusan PGSD dengan 3 *host*. Kedua VLAN ini akan dihubungkan dengan topologi jaringan yang sudah ada sebelumnya menggunakan kabel *Cross-Over*. Pemilihan kabel *Cross-Over* ini penting karena menghubungkan dua perangkat yang sejenis, yaitu *switch* ke *switch*.

ISSN (e): 2540-9123
ISSN (p): 2502-1982



Gambar 7. Topologi *case* 2.

Setelah perancangan topologi selesai, proses berlanjut ke tahap implementasi. Pada tahap ini, setiap *host* baru perlu dikonfigurasi dengan alamat IP yang sesuai dengan kelompok VLAN-nya masing-masing. *Host-host* dalam VLAN 10 (SISTEL) akan menggunakan IP dengan subnet yang sama dengan VLAN 10 pada topologi sebelumnya, begitu juga dengan *host-host* dalam VLAN 20 (PGSD). Selain konfigurasi IP, *port interfaces* pada *switch* juga perlu dikonfigurasi untuk menentukan port mana yang akan terhubung ke *host* mana dan VLAN mana. Proses ini dapat divisualisasikan seperti yang terdapat dalam Gambar 8.

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name SISTEL
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name PGSD
Switch(config-vlan)#exit
Switch(config)#interface range fa 0/11 -12
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range fa 0/13 -15
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                 Gig0/2
10   SISTEL                            active    Fa0/11, Fa0/12
20   PGSD                              active    Fa0/13, Fa0/14, Fa0/15
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Gambar 8. Konfigurasi *case* 2.

Langkah krusial terdapat dalam Gambar 9. yang merupakan tahap aktivasi mode *trunk* pada *port* yang menghubungkan kedua *switch*. Mode *trunk* ini memungkinkan lalu lintas data dari berbagai VLAN dapat melewati satu jalur fisik yang sama antara kedua *switch*.

ISSN (e): 2540-9123
ISSN (p): 2502-1982

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fa 0/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#show interface fastEthernet 0/2 switchport
```

Gambar 9. Aktivasi mode *trunk.*

3. Hasil dan Pembahasan

3.1 Uji Konektivitas Antar Perangkat

Pada Gambar 10. Menampilkan proses uji konektivitas yang berhasil dikirim ke alamat IP 192.168.30.1 dengan paket data berukuran 32 byte. Kemudian menampilkan pula balasan (*reply*) yang diterima dari perangkat yang di-*ping*. Balasan tersebut mencakup informasi jumlah byte data, waktu respons, dan *Time to Live* (TTL) paket. Di baris terakhir, terdapat statistik lengkap mengenai perintah *ping* yang telah dilakukan. Statistik tersebut mencakup jumlah paket yang terkirim, diterima, dan hilang, serta waktu minimum, maksimum, dan rata-rata respons.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time=22ms TTL=128
Reply from 192.168.30.1: bytes=32 time<1ms TTL=128
Reply from 192.168.30.1: bytes=32 time<1ms TTL=128
Reply from 192.168.30.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 22ms, Average = 5ms
```

Gambar 10. Uji konektivitas antar perangkat.

3.2 Pengujian Interface Mode Trunk

Pada bagian ini disajikan hasil pengujian untuk memastikan konfigurasi telah berhasil. Pada Gambar 11. pengujian dimulai dengan memverifikasi *interface trunk* pada *Command Line Interface (CLI) switch.*

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fa 0/2
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

Switch(config-if)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show interface fastEthernet 0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Gambar 11. Verifikasi *interface trunk.*

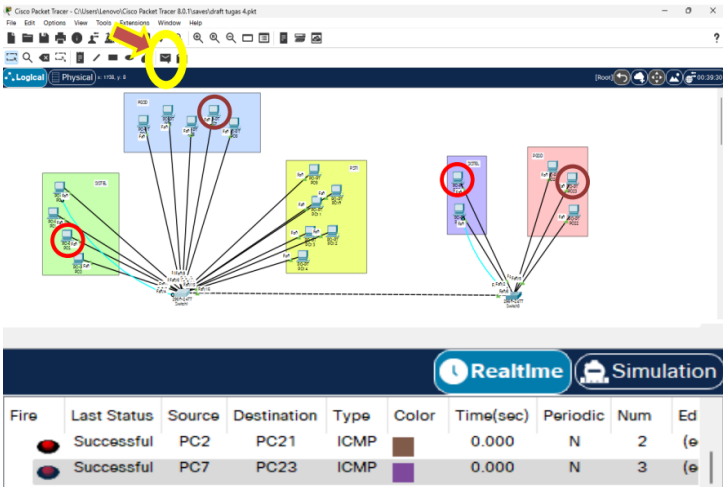
ISSN (e): 2540-9123
ISSN (p): 2502-1982

Gambar tersebut menampilkan detail konfigurasi *switchport* pada antarmuka *FastEthernet0/2*. Informasi yang ditampilkan mencakup status *switchport* yang diaktifkan, mode administrasi yang diatur sebagai trunk, enkapsulasi *trunk* yang menggunakan *dot1q*, dan berbagai pengaturan VLAN lainnya. Selain itu, tampilan juga menunjukkan informasi terkait mode operasional, status VLAN, dan fitur-fitur keamanan yang dikonfigurasi pada *switch* tersebut. Secara umum, detail konfigurasi yang ditampilkan mencerminkan upaya untuk mengatur dan mengoptimalkan perilaku *switch* dalam lingkungan jaringan.

3.3 Pengujian VLAN Trunking

Perintah ini akan menampilkan status dan konfigurasi dari port yang telah diatur sebagai *trunk*. Selanjutnya, dilakukan pengujian konektivitas antar VLAN yang berada pada *switch* yang berbeda. Pengujian ini dilakukan untuk memastikan bahwa *host* dalam VLAN yang sama namun berada pada *switch* yang berbeda dapat saling berkomunikasi, walaupun tetap terisolasi dari VLAN yang berbeda. Selain itu, isolasi VLAN juga berperan penting dalam aspek keamanan jaringan. Dengan adanya segmentasi logis, VLAN dapat membatasi akses antar divisi atau kelompok kerja sehingga jika terjadi serangan pada satu VLAN, dampaknya tidak langsung menyebar ke seluruh jaringan. Misalnya, dalam kasus serangan ARP *spoofing* di jaringan rumah sakit, perangkat yang terinfeksi hanya memengaruhi VLAN tertentu, sementara VLAN lain seperti VLAN administrasi atau VLAN server tetap terlindungi. Studi oleh ElShafee dan El-Shafai (2023) menunjukkan bahwa isolasi jaringan mampu meminimalisasi potensi data link impersonation attack yang dapat mengekspos layanan aplikasi pada LAN tradisional [13]. Contoh nyata lainnya ditemukan pada implementasi VLAN di sektor pendidikan, di mana VLAN digunakan untuk memisahkan jaringan dosen, mahasiswa, dan administrasi. Jika salah satu jaringan mahasiswa disusupi *malware* melalui perangkat pribadi, VLAN mencegah lalu lintas berbahaya tersebut menjalar ke *server* akademik yang berada pada VLAN berbeda. Hal ini memperkuat argumen bahwa isolasi VLAN tidak hanya berdampak pada efisiensi kinerja, tetapi juga merupakan lapisan keamanan preventif yang efektif [14].

Keberhasilan pengujian ditandai dengan status "*Successful*" pada saat melakukan *PING* antar *host* dalam VLAN yang sama meskipun berada pada *switch* yang berbeda seperti yang terdapat dalam Gambar 12 yakni dengan menghubungkan PC 2 dengan PC 21 (Lingkaran Merah) dan PC 7 dengan PC 23 (Lingkaran Coklat) kemudian untuk mengirim sinyal menggunakan *Add Simple PDU* (Lingkaran Kuning)



Gambar 12. Pengujian VLAN *trunking.*

Prosedur ini memastikan bahwa meskipun jaringan secara fisik terpisah pada dua *switch* yang berbeda, *host-host* dalam VLAN yang sama tetap dapat berkomunikasi seolah-olah berada dalam satu jaringan lokal yang sama, sementara tetap mempertahankan isolasi dari VLAN lainnya. Hal ini mendemonstrasikan salah satu keunggulan utama dari teknologi VLAN dalam

ISSN (e): 2540-9123
ISSN (p): 2502-1982

manajemen jaringan modern. Dengan VLAN, administrator jaringan memiliki fleksibilitas untuk mengelola dan mengubah jaringan sesuai kebutuhan tanpa harus mengubah kabel fisik [14]. Hal ini sangat bermanfaat dalam organisasi besar di mana sering terjadi perubahan struktur atau penambahan perangkat. VLAN memungkinkan organisasi untuk menyesuaikan pengaturan jaringan secara logis dan efisien. Misalnya, jika VLAN digunakan untuk membatasi akses perangkat yang tidak relevan ke data perusahaan, ini dapat menjadi langkah pengamanan penting dalam melindungi data dari akses tidak sah.

3.4 Hasil Analisis Kinerja VLAN

Selain pengujian fungsional berupa *ping test* dan verifikasi konfigurasi *trunk*, penelitian ini juga melakukan pengukuran parameter kinerja jaringan untuk memberikan gambaran lebih objektif mengenai performa VLAN. Tiga parameter utama yang diuji adalah *latency*, *throughput*, dan *packet loss*. Pengukuran dilakukan dalam tiga skenario utama yaitu Case 1 (*VLAN* tanpa *trunking*), case 2 (VLAN dengan *trunking*), dan komunikasi antar *VLAN* tanpa izin serta antar VLAN dengan *trunking*.

Tabel 1. Hasil pengujian kinerja jaringan VLAN.

Skenario	Rata-rata Latency (ms)	Throughput (kbps)	Packet Loss (%)
Case 1 (VLAN tanpa *trunking*)	5.2	980	0
Case 2 (VLAN dengan *trunking*)	6.8	950	0
Antar VLAN (dengan *trunking*)	7.1	940	0

Menurut Tabel 1. menunjukkan nilai rata-rata *latency* antara 5.2 ms (intra-VLAN tanpa *trunking*) hingga 7.1 ms (inter-VLAN dengan *trunking*), *throughput* pada kisaran 940–980 kbps, serta *packet loss* mendekati 0% untuk komunikasi yang diizinkan. Nilai-nilai ini konsisten dengan prinsip dasar VLAN yaitu segmentasi domain siaran (*broadcast* domain) dapat mengurangi *delay* dan kehilangan paket sehingga meningkatkan keandalan komunikasi pada jaringan lokal [16]. Beberapa studi sebelumnya juga melaporkan bahwa penerapan VLAN dapat menurunkan *delay* dan paket yang hilang pada jaringan yang tadinya satu domain siaran besar [15]. Temuan serupa [16] dilaporkan oleh penelitian simulasi dan studi kasus yang menunjukkan peningkatan performa jaringan (*delay* dan *packet loss*) setelah diterapkan VLAN pada topologi yang sesuai. Namun, beberapa kondisi *throughput* dapat mengalami penurunan kecil setelah segmentasi karena *overhead* tambahan dan mekanisme *forwarding* tertentu [16].

Kenaikan *latency* yang teramati pada skenario *trunking* (6.8 ms dan 5.2 ms) terjadi karena adanya proses *tagging* IEEE 802.1Q pada paket yang melewati *trunk*, pemrosesan tambahan pada *port trunk*, serta kemungkinan jalur *forwarding* yang lebih panjang (lebih banyak *hop logical*) dibandingkan komunikasi intra-*switch*. Adapun menurut penelitian [17] bahwa kondisi *throughput* yang sedikit menurun pada konfigurasi *trunking* (dari 980 kbps menjadi 950/940 kbps) selaras dengan penelitian simulasi yang menyatakan bahwa VLAN berfungsi lebih pada segmentasi dan pengurangan *broadcast* daripada meningkatkan kapasitas *throughput* intrinsik jaringan.

4. Kesimpulan

Berdasarkan hasil implementasi dan konfigurasi VLAN menggunakan Cisco *Packet Tracer*, dapat disimpulkan bahwa penerapan VLAN efektif meningkatkan efisiensi sekaligus keamanan jaringan lokal. Hasil pengujian menunjukkan bahwa *latency* tetap rendah (<10 ms) meskipun terdapat kenaikan sebesar 30–36% saat menggunakan *trunking* dibandingkan VLAN dasar. Sementara itu, *throughput* tetap stabil di atas 900 kbps, dengan hanya mengalami penurunan kecil sekitar 3–4% akibat *overhead tagging* IEEE 802.1Q. Selain itu, *packet loss* tercatat 0% pada

seluruh skenario, yang berarti tidak ada degradasi keandalan transmisi data. Dengan demikian, VLAN terbukti mampu menurunkan *broadcast traffic*, menjaga kualitas komunikasi antar perangkat, serta mendukung fleksibilitas manajemen jaringan. Hasil ini menunjukkan bahwa konfigurasi VLAN dapat memberikan optimalisasi nyata terhadap jaringan lokal, baik dari sisi efisiensi (penurunan *broadcast traffic*), performa (*latency* dan *throughput* terjaga), maupun keamanan (isolasi lalu lintas antar VLAN)

Referensi

[1] M. Martias, Azhari, Ardy, and D. Saputra, "Penerapan Jaringan Virtual Local Area Network Dengan Cisco Packet Tracer," pp. 28–33, 2020. [Online]. Available: https://www.semanticscholar.org/paper/17bb3ad180e5a95ed38a87eb18e743b04cd9a614

[2] T. Rahman, T. R. Zaini, and G. Chrisnawati, "Perancangan Jaringan Virtual Local Area Network (VLAN) & DHCP Pada PT. Navicom Indonesia Bekasi," JIKA (Jurnal Informatika), 2020, doi: 10.31000/JIKA.V4I1.2366.

[3] B. B. Yoga and M. A. Raharja, "Implementasi VLAN (Virtual Local Area Network) pada Rumah Sakit Mata Ramata," JELIKU (Jurnal Elektronik Ilmu Komputer Udayana), 2019, doi: 10.24843/jlk.2019.v07.i03.p07.

[4] R. Salam and Jenih, "Perancangan dan Implementasi VLAN dengan VLAN Trunking Protocol (VTP) di PT. Citra Solusi Pratama," Jurnal Teknologi Informasi, vol. 8, no. 2, pp. 1–7, 2022, doi: 10.52643/jti.v8i2.2722.

[5] O. J. Usior and E. Sediyono, "Simulasi Extended ACL pada Jaringan VLAN Menggunakan Aplikasi Cisco Packet Tracer," AITI, vol. 20, no. 1, pp. 32–47, 2023, doi: 10.24246/aiti.v20i1.32-47.

[6] S. Surono, F. W. Christanto, and C. Maulana, "Uji Komparasi Quality of Service Antara Metode Routing dan VLAN pada Distribusi Paket Data Jaringan Internet," Jurnal Pengembangan Rekayasa dan Teknologi, vol. 16, no. 2, pp. 45–53, 2021, doi: 10.26623/jprt.v16i2.3058.

[7] A. R. Maulana et al., "Optimalisasi Jaringan IPv4 pada Local Area Network (LAN) di Perusahaan," Digital Transformation Technology, vol. 4, no. 1, pp. 1–10, 2024, doi: 10.47709/digitech.v4i1.3983.

[8] Fatkhurrahman and A. Witanti, "Optimasi Segmentasi Jaringan melalui Implementasi VLAN Dinamis pada Infrastruktur Kabel dan Nirkabel dengan MikroTik," JEKIN – Jurnal Teknik Informatika, vol. 4, no. 3, pp. 1–9, 2024, doi: 10.58794/jekin.v4i3.904.

[9] A. ElShafee and W. El-Shafai, "Design and analysis of data link impersonation attack for wired LAN application layer services," Journal of Ambient Intelligence and Humanized Computing, vol. 14, no. 2, pp. 987–995, 2023, doi: 10.1007/s12652-022-03800-5.

[10] A. Noviriandini, D. Bachtiar, and L. Indriyani, "Perancangan Jaringan Virtual Local Area Network Menggunakan Cisco Packet Tracer pada SMK Islam Assa'adatul Abadiyah," JUKI: Jurnal Komputer, vol. 5, no. 2, pp. 100–108, 2023, doi: 10.53842/juki.v5i2.389.

[11] N. Musyaffa and R. Sastra, "Implementasi Access Inter-VLAN Menggunakan Router," INSANtek – Jurnal Inovasi dan Sains Teknik Elektro, vol. 4, no. 1, pp. 15–20, 2020.

[12] H. Harjono and A. P. Wicaksono, "Simulasi Virtual Local Area Network Menggunakan Packet Tracer," Sainteks, vol. 15, no. 2, pp. 1–6, 2020, doi: 10.30595/sainteks.v15i2.6315.

[13] H. Ar-Rasyid, S. Broto, and W. Artika, "Optimasi Infrastruktur Jaringan VLAN Trunking Protocol Menggunakan Simulasi Packet Tracer pada PT. Rukun Sejahtera Teknik," JEIS: Jurnal Elektro dan Sistem, vol. 4, no. 1, pp. 20–28, 2024, doi: 10.56486/jeis.vol4no1.422.

[14] R. Salam and J. Jenih, "Perancangan dan Implementasi VLAN dengan VLAN Trunking Protocol (VTP) di PT. Citra Solusi Pratama," Jurnal Teknologi Informasi, vol. 8, no. 2, pp. 1–7, 2022, doi: 10.52643/jti.v8i2.2722.

[15] A. I. Cahyando, R. Andriani, R. Pahlipi, et al., "Penerapan Teknik VLAN Untuk Mengoptimalisasi Kirim Data," Intechno Journal, vol. 3, no. 2, pp. 55–63, 2021, doi: 10.24076/intechnojournal.2021v3i2.1555.

[16] S. Surono, F. W. Christanto, and C. Maulana, "Uji Komparasi Quality of Service Antara Metode Routing dan VLAN pada Distribusi Paket Data Jaringan Internet," Jurnal Pengembangan Rekayasa dan Teknologi, vol. 16, no. 2, pp. 45–53, 2021.

[17] A. ElShafee and W. El-Shafai, "Design and analysis of data link impersonation attack for wired LAN application layer services," Journal of Ambient Intelligence and Humanized Computing, vol. 14, no. 2, pp. 987–995, 2023, doi: 10.1007/s12652-022-03800-5.