Jurnal Sains Informatika Terapan (JSIT)
E-ISSN: 2828-1659, Volume: 4, Issue: 2, Month: Juny, Year: 2025
Page: 264-270, Available online at: https://rcf-indonesia.org/home/

ANALISIS KEAMANAN DAN KINERJA JARINGAN PADA IMPLEMENTASI VLAN SEBAGAI UPAYA SEGMENTASI TRAFIK MENGGUNAKAN CISCO PACKET TRACER

Sunarsan Sitohang[1)], Hotma Pangaribuan[2)]
[1]Teknik Informatika Universitas Putera Batam
[2] Teknik Informatika Universitas Putera Batam
Corresponding Author: [1] sunarsan@puterabatam.ac.id

Article Info

Article history:

Received: Mei 10, 2025
Revised: Juny 10, 2025
Accepted: Juny 20, 2025
Published: Juny 30, 2025

Keywords:

VLAN
Switch
Cisco Packet Tracer
Trafik
Jaringan Komputer

ABSTRAK

Dalam era digital saat ini, kebutuhan akan jaringan komputer yang andal, efisien, dan aman semakin meningkat, terutama pada organisasi yang memiliki banyak departemen dan perangkat yang saling terhubung. Untuk menjawab tantangan tersebut, konsep *Virtual Local Area Network* (VLAN) merupakan salah satu solusi yang digunakan secara luas dalam arsitektur jaringan modern. Switch sebagai perangkat Dimana akan diterapkannya vlan dengan mode access dan trunk. *Cisco Packet Tracer* merupakan perangkat lunak yang dapat digunakan dalam mensimulasikan penerapan vlan untuk melakukan segmentasi trafik. Simulasi sebagai metode yang dipilih dikarenakan sangat memudahkan untuk memahami jaringan baik untuk pembelajaran maupun untuk melihat detail dari setiap konfigurasi. Simulasi ini dilakukan pada tiga *switch* dan tiga vlan id yaitu Vlan 10, 20, 30 memisahkan ruang guru, lab akutansi dan lab rekayasa perangkat lunak. Berdasarkan hasil pengujian simulasi konfigurasi vlan berjalan dengan baik dilihat dari antarvlan yang berbeda terblok komunikasinya sedangkan untuk yang sama vlannya aksesnya sukses. Dengan segmentasi yang telah diterapkan menciptakan keamanan jaringan yang lebih baik sebelumnya yaitu tanpa adanya penerapan vlan

1. PENDAHULUAN

Dalam era digital saat ini, kebutuhan akan jaringan komputer yang andal, efisien, dan aman semakin meningkat, terutama pada organisasi yang memiliki banyak departemen dan perangkat yang saling terhubung. Salah satu tantangan utama dalam pengelolaan jaringan adalah bagaimana menyegmentasi lalu lintas data untuk meningkatkan keamanan dan kinerja tanpa harus menambah perangkat keras secara berlebihan. Instansi atau organisasi maupun sekolah hendaknya berusaha untuk meminimalisir pengeluaran sehingga dengan biaya rendah maka operasional instansi atau organisasi maupun sekolah akan berjalan optimal. Dijaman digitalisasi saat ini semua hendaknya disediakan secara baik, mudah dan aman serta memberikan setidaknya tiga elemen dasar dari keamanan jaringan yaitu *confidentially*, *integrity* dan *availability* [1].

Salah satu tantangan utama yang dihadapi dalam manajemen jaringan adalah segmentasi lalu lintas data antar departemen. Tanpa adanya segmentasi yang tepat, seluruh perangkat dalam jaringan dapat saling berkomunikasi secara bebas. Hal ini berisiko menimbulkan kemacetan lalu lintas jaringan (*network congestion*), celah keamanan (*security loophole*), dan kesulitan dalam manajemen trafik serta *troubleshooting*. Solusi tradisional seperti penggunaan switch atau router terpisah untuk setiap divisi tentu tidak efisien, karena akan menambah beban biaya dan kompleksitas perangkat keras.

Untuk menjawab tantangan tersebut, konsep Virtual Local Area Network (VLAN) merupakan salah satu solusi yang digunakan secara luas dalam arsitektur jaringan modern [2]. Dengan VLAN, administrator jaringan dapat membagi satu jaringan fisik menjadi beberapa segmen logis yang terpisah. Hal ini tidak hanya mempermudah manajemen jaringan, tetapi juga meningkatkan keamanan dengan membatasi lalu lintas antar departemen atau kelompok kerja [3], [4]. Melalui VLAN, perangkat yang secara fisik terhubung ke switch yang sama dapat ditempatkan dalam segmen jaringan yang berbeda secara logis, tergantung pada fungsinya atau lokasi kerjanya. Dengan demikian, VLAN tidak hanya membantu dalam pengelolaan jaringan yang lebih sistematis, tetapi juga meningkatkan keamanan dengan membatasi lalu lintas antar pengguna yang

tidak relevan, serta mengurangi *broadcast domain* yang dapat mengganggu performa jaringan.

Namun, meskipun VLAN menawarkan banyak keuntungan, implementasinya juga menimbulkan pertanyaan mengenai seberapa efektif VLAN dalam meningkatkan keamanan dan kinerja jaringan secara nyata [5],[6]. Misalnya, masih terdapat potensi serangan seperti VLAN hopping jika konfigurasi dilakukan secara tidak tepat [7], [1]. Dimana seorang penyerang mencoba untuk mengakses VLAN lain yang seharusnya tidak dapat diakses, dengan memanfaatkan kelemahan dalam konfigurasi trunking dan pengaturan native VLAN [8], [9], [10]. Selain itu, segmentasi jaringan yang berlebihan atau tidak terstruktur juga berpotensi menimbulkan *bottleneck* dalam komunikasi antar VLAN, terutama jika tidak diimbangi dengan inter-VLAN routing yang baik. Selain itu, perlu dilakukan analisis terhadap dampak segmentasi VLAN terhadap kecepatan dan efisiensi komunikasi jaringan [11], [12], [13]

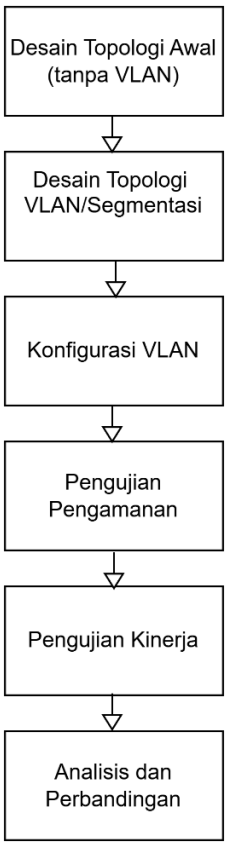
Oleh karena itu, perlu dilakukan kajian mendalam untuk menjawab pertanyaan-pertanyaan berikut: Sejauh mana efektivitas VLAN dalam meningkatkan keamanan dan performa jaringan?, Bagaimana dampak segmentasi logis VLAN terhadap efisiensi lalu lintas data dan pengendalian akses?, Apa konfigurasi optimal VLAN agar dapat mencegah celah keamanan tanpa mengorbankan kinerja jaringan?

Penelitian ini dilakukan untuk menganalisis implementasi VLAN pada jaringan komputer multidepartemen dengan pendekatan simulasi menggunakan *Cisco Packet Tracer*. *Cisco Packet Tracer* dipilih karena merupakan salah satu perangkat lunak simulasi jaringan yang luas digunakan di dunia pendidikan dan pelatihan profesional. Melalui simulasi ini, peneliti akan merancang topologi jaringan dengan dan tanpa VLAN, kemudian mengamati perbedaan kinerja jaringan (respons waktu, *broadcast*, efisiensi trafik) serta tingkat isolasi antar segmen jaringan. Selain itu, penelitian juga akan mengevaluasi bagaimana konfigurasi tambahan seperti inter-VLAN routing dan access control list (ACL) dapat meningkatkan efisiensi sekaligus keamanan jaringan [3].

Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi dalam bentuk pemahaman teoretis dan praktis mengenai manfaat, tantangan, dan penerapan VLAN dalam lingkungan jaringan nyata, khususnya dalam konteks organisasi yang membutuhkan segmentasi jaringan yang efektif dan aman. Menggunakan *Cisco Packet Tracer* sebagai media simulasi, penelitian ini bertujuan untuk memberikan pemahaman praktis dan teoritis mengenai konfigurasi VLAN yang baik dan benar, serta mengevaluasi performa jaringan sebelum dan sesudah VLAN diterapkan.

2. METODE PENELITIAN

Penelitian analisis keamanan dan kinerja jaringan pada implementasi VLAN menggunakan metode Kuantitatif eksperimental menggunakan simulasi cisco paket tracer. Berikut gambar 1 merupakan tahapan-tahapannya.



Gambar 1. Tahapan Penelitian

Berikut adalah penjelasan dari gambar 1 diatas:

Desain Topologi Awal (Tanpa VLAN)

Peneliti mensimulasikan topologi jaringan awal yang tidak menerapkan VLAN. Didalam topologi ini secara teori dinyatakan dengan Semua perangkat dalam satu *broadcast domain* [14] [15].

Desain Topologi VLAN (Setelah Segmentasi)

Mensimulasikan topologi jaringan baru dan menerapkan VLAN untuk menggantikan topologi awal. Topologi jaringan baru ini menerapkan pembuatan segmentasi atau membuat VLAN terpisah untuk tiap departemen/bagian.

Konfigurasi VLAN

Untuk penerapan VLAN maka menggunakan switch dan VLAN ID, membuat dan memberi nama VLAN, membuat antarmuka manajemen/ *Switch Virtual Interface* (SVI), Tentukan port mana yang tergabung ke VLAN tertentu serta Untuk koneksi antar switch.

Pengujian Keamanan

Mensimulasikan percobaan komunikasi antar VLAN tanpa router atau ACL sebagai ilustrasi kontrol akses.

Pengujian Kinerja

Pengukuran Bandwidth dan latency menggunakan tools dalam Packet Tracer yaitu simulation mode, traffic generator, ping response time.

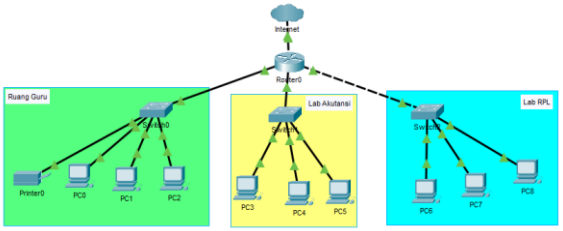
Analisis dan Perbandingan

Membandingkan performa dan keamanan antara jaringan tanpa VLAN dan dengan VLAN.

3. HASIL DAN PEMBAHASAN

3.1 Desain Topologi Awal

Berikut gambar 2 adalah gambaran rancagan jaringan yang sedang digunakan, dimana tidak diterapkannya Vlan. Terdapat tiga switch yaitu switch diruang guru, ruangan laboratorium SMK jurusan Akutansi dan Laboratorium SMK jurusan rekayasa perangkat lunak.



Gambar 2. Topologi Jaringan lama

3.2 Desain Topologi Jaringan VLAN

Penelitian ini menggunakan dua topologi untuk dibandingkan, yaitu:

a. Topologi Tanpa VLAN (Baseline): Semua perangkat berada dalam satu jaringan tanpa segmentasi. Komunikasi antar semua host diperbolehkan, dan topologi ini adalah jaringan yang sedang berjalan.

b. Topologi Dengan VLAN: Jaringan dibagi menjadi 6 VLAN yaitu VLAN 10, 20, 30, 40, 99 dan 100 dan topologi ini yang coba diajukan untuk diterapkan dan pada penelitian ini menyuguhkan berupa simulasi sebagai sesuatu yang akan diusulkan.

Untuk mengimplementasikan VLAN dibutuhkan daftar VLAN yang akan dikonfigurasi serta Alamat ip dimasing-masing perangkat akhir yang tertera pada tabel 1 dan tabel 2 dibawah ini.

Tabel 1. VLAN

No VLAN	Nama VLAN
10	Guru
20	Lab-Akunt
30	Lab-RPL

Tabel 2. Pengalamatan

Perangkat	Interface	Alamat	Subnet Mask	Switchport	VLAN
RG1	NIC	192.168.10.10	255.255.255.0	SW-Guru	VLAN 10
RG2	NIC	192.168.20.20	255.255.255.0	SW-Guru	VLAN 20
RG3	NIC	192.168.30.30	255.255.255.0	SW-Guru	VLAN 30
AK1	NIC	192.168.10.11	255.255.255.0	SW-Aki	VLAN 10
AK2	NIC	192.168.20.21	255.255.255.0	SW-Ak	VLAN 20
AK3	NIC	192.168.30.31	255.255.255.0	SW-AK	VLAN 30
RPL1	NIC	192.168.10.12	255.255.255.0	SW-RPL	VLAN 10
RPL2	NIC	192.168.20.22	255.255.255.0	SW-RPL	VLAN 20
RPL3	NIC	192.168.30.32	255.255.255.0	SW-RPL	VLAN 30
PC4	NIC	192.168.20.23	255.255.255.0	SW-Akutansi	VLAN 20
SW Guru	SVI	192.168.99.252	255.255.255.0	N/A	VLAN 99
SW Akunt	SVI	192.168.99.252	255.255.255.0	N/A	VLAN 99
SW RPL	SVI	192.168.99.252	255.255.255.0	N/A	VLAN 99

3.3 Konfigurasi VLAN

1. Mendaftarkan VLAN

Tahap ini peneliti akan mengkonfigurasikan VLAN di tiga switch yaitu switch Guru, Lab-Ak dan Lab-RPL. Tiap-tiap switch akan didaftarkan tiga ID VLAN yaitu VLAN 10, 20 dan 30 dan hasil konfigurasinya tertera pada gambar 3, 4, 5 dibawah ini.

```
Switch(config)#hostname SW-Guru
SW-Guru(config)#vlan 10
SW-Guru(config-vlan)#name Guru
SW-Guru(config-vlan)#vlan 20
SW-Guru(config-vlan)#name Lab-Akunt
SW-Guru(config-vlan)#vlan 30
SW-Guru(config-vlan)#name Lab-RPL
SW-Guru(config-vlan)#vlan 40
SW-Guru(config-vlan)#name Voice
SW-Guru(config-vlan)#vlan 99
SW-Guru(config-vlan)#name Management
SW-Guru(config-vlan)#vlan 100
SW-Guru(config-vlan)#name Native
SW-Guru(config-vlan)#
```

Gambar 3. Konfigurasi SW-Guru

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname RPL
RPL(config)#vlan 10
RPL(config-vlan)#name guru
RPL(config-vlan)#vlan 20
RPL(config-vlan)#name Lab-Akunt
RPL(config-vlan)#vlan 30
RPL(config-vlan)#name Lab-RPL
RPL(config-vlan)#vlan 99
RPL(config-vlan)#name Management
RPL(config-vlan)#vlan 100
RPL(config-vlan)#name Native
RPL(config-vlan)#exit
RPL(config)#exit
RPL#
```

Gambar 4. Konfigurasi SW-RPL

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Ak
Ak(config)#vlan 10
Ak(config-vlan)#name guru
Ak(config-vlan)#vlan 20
Ak(config-vlan)#name Lab-Akunt
Ak(config-vlan)#vlan 30
Ak(config-vlan)#name Lab-RPL
Ak(config-vlan)#vlan 99
Ak(config-vlan)#name Management
Ak(config-vlan)#vlan 100
Ak(config-vlan)#name Native
Ak(config-vlan)#exit
Ak(config)#
Ak(config)#exit
```

Gambar 5. Konfigurasi SW-AK

Setelah mendaftarkan VLAN ke Switch maka kita dapat verifikasi apakah VLAN sudah terdaftar dengan benar menggunakan perintah "Switch#Show VLAN". Dan hasil konfigurasinya tertera pada gambar 6, 7 dan 8 dibawah ini.

```
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   guru                             active
20   Lab-Akunt                        active
30   Lab-RPL                          active
99   Management                       active
100  Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Gambar 6. Hasil Konfigurasi Sw-Guru

```
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   guru                             active
20   Lab-Akunt                        active
30   Lab-RPL                          active
99   Management                       active
100  Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Gambar 7. Hasil Konfigurasi Sw-AK

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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   guru                             active    Fa0/1
20   Lab-Akunt                        active    Fa0/2
30   Lab-RPL                          active    Fa0/3
99   Management                       active
100  Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Gambar 8. Hasil Konfigurasi Sw-RPL

2. Konfigurasi *Interface Switch Mode Acces*

Setiap *interface switch* akan dikonfigurasikan mode aksesnya, *interface* yang dimaksudkan adalah i*nterfase* yang terhubung ke*host* sesuai rencana yang telah dibuat. Interface fastethernet 0/1, 0/2 serta 0/3 diatur kemode access serta diarah ke VLAN yang dirancanakan seperti gambar 8, 9 dibawah ini

```
RPL>
RPL>en
RPL#config t
Enter configuration commands, one per line.  End with CNTL/Z.
RPL(config)#int fa0/1
RPL(config-if)#switchport mode access
RPL(config-if)#switchport access vlan 10
RPL(config-if)#exit
RPL(config)#int fa0/2
RPL(config-if)#switchport mode access
RPL(config-if)#switchport access vlan 20
RPL(config-if)#exit
RPL(config)#int fa0/3
RPL(config-if)#switchport mode access
RPL(config-if)#switchport access vlan 30
RPL(config-if)#exit
```

Gambar 8. Konfigurasi interface ke Mode Acces dan VLAN SW-RPL

```
Ak>
Ak>en
Ak#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Ak(config)#int fa0/1
Ak(config-if)#switchport mode access
Ak(config-if)#switchport access vlan 10
Ak(config-if)#exit
Ak(config)#int fa0/2
Ak(config-if)#switchport mode access
Ak(config-if)#switchport access vlan 20
Ak(config-if)#exit
Ak(config)#int fa0/3
Ak(config-if)#switchport mode access
Ak(config-if)#switchport access vlan 30
Ak(config-if)#exit
Ak(config)#exit
Ak#show vlan
```

Gambar 9. Konfigurasi interface ke Mode Acces dan VLAN SW-Ak

Untuk menhubungkan perangkat VLAN yang sama antar *switch* maka dimasing-masing *interface swich* harus dikonfigurasi dengan mode *trunk*, pada *switch* SW-guru *interface* gigabitethernet 0/1 terhubung dengan interface gigabitethernet 0/1 SW-Ak serta *interface* gigabitethernet 0/2 terhubung dengan gigabitethernet 0/1 SW-RPL. Kelima interface di tiga switch ini dikonfigurasi kedalam mode trunk seperti terlihat pada gambar dibawah ini.

```
SW-Guru#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-Guru(config)#int gig0/1
SW-Guru(config-if)#switchport mode trunk
```

Gambar 10 (a) Konfigurasi Mode Trunk SW-Guru

```
Ak#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Ak(config)#int gig0/1
Ak(config-if)#switchport mode trunk
Ak(config-if)#exit
Ak(config)#int gig0/2
Ak(config-if)#switchport mode trunk
```

Gambar 10 (b) Konfigurasi Mode Trunk SW-Ak

```
RPL#config t
Enter configuration commands, one per line.  End with CNTL/Z.
RPL(config)#int gig0/1
RPL(config-if)#switchport mode trunk
```

Gambar 10 (C) Konfigurasi Mode Trunk SW-RPL

Setelah melakukan konfigurasi, selanjutnya melakukan verifikasi, dan hasilnya sseperti gambar 11 dibawah ini.

```
SW-Guru#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,10,20,30,40,99,100

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,10,20,30,40,99,100
```

Gambar 11 (a) Verifikasi Mode Trunk SW-Guru

```
Ak#show in
Ak#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1
Gig0/2      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,10,20,30,99,100
Gig0/2      1,10,20,30,99,100

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,10,20,30,99,100
Gig0/2      1,10,20,30,99,100
```

Gambar 11 (b) Verifikasi Mode Trunk SW-Ak

```
RPL#show int
RPL#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,10,20,30,99,100

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,10,20,30,99,100
```

Gambar 11 (c) Verifikasi Mode Trunk SW-RPL

3.4 Pengujian Keamanan: Isolasi Antar VLAN

1. Pengujian Tanpa VLAN

Pada jaringan tanpa VLAN, semua PC dapat melakukan komunikasi dengan bebas menggunakan perintah ping terlihat seperti gambar 12. Tidak ada pemisahan lalu lintas antar departemen. Hasil pengujian sebelum inisiasi VLAN bahwa antar perangkat dalam satu switch tidak dapat terhubung dikarenakan pengaturan ipnya berbeda jaringan.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic
	In Progress	RG1	RG2	ICMP		0.000	N
	In Progress	RG2	RG3	ICMP		0.000	N
	In Progress	RG1	RG3	ICMP		0.000	N

Gambar 12 Status Koneksi Tanpa Inisiasi Vlan

2. Pengujian Dengan VLAN

Tabel 3 berikut adalah hasil pengujian akses Vlan dengan mode realtime, berdasarkan hasil pengujian antar Vlan yang sama di*switch* berbeda berstatus *success*, sedangkan antara berbeda Vlan di*switch* yang sama maupun di*switch* berbeda berstatus *request time out* (RTO) atau di "*block*".

Tabel 3. Ringkasan Hasil Pengujian

SW-Guru/ SW-AK	RG1 Vlan 10	RG2 Vlan 20	RG3 Vlan 30
Ak-1 Vlan 10	Success	RTO	RTO
Ak-2 Vlan 20	RTO	Success	RTO
Ak-3 Vlan 30	RTO	RTO	Success
SW-Guru/ SW-RPL	RG1 Vlan 10	RG2 Vlan 20	RG3 Vlan 30
RPL-1 Vlan 10	Success	RTO	RTO
RPL-2 Vlan 20	RTO	Success	RTO
RPL-3 Vlan 30	RTO	RTO	Success
SW-RPL/ SW-AK	RPL-1 Vlan 10	RPL-2 Vlan 20	RPL-3 Vlan 30
Ak-1 Vlan 10	Success	RTO	RTO
Ak-2 Vlan 20	RTO	Success	RTO
Ak-3 Vlan 30	RTO	RTO	Success

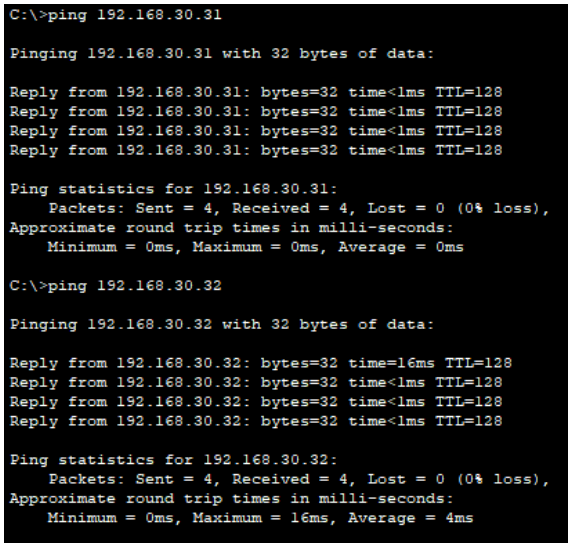
Selain pengujian mode *realtime*, dilakukan juga pengujian *ping respon time* yang tertera pada gambar 12, 13, 14 dibawah ini.

```
C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.12

Pinging 192.168.10.12 with 32 bytes of data:

Reply from 192.168.10.12: bytes=32 time<1ms TTL=128
Reply from 192.168.10.12: bytes=32 time<1ms TTL=128
Reply from 192.168.10.12: bytes=32 time=1ms TTL=128
Reply from 192.168.10.12: bytes=32 time=10ms TTL=128

Ping statistics for 192.168.10.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

Gambar 13 Hasil Test Koneksi dari PC-RG1 ke PC-AK1 dan PC-RPL1

```
C:\>ping 192.168.20.22

Pinging 192.168.20.22 with 32 bytes of data:

Reply from 192.168.20.22: bytes=32 time<1ms TTL=128
Reply from 192.168.20.22: bytes=32 time<1ms TTL=128
Reply from 192.168.20.22: bytes=32 time<1ms TTL=128
Reply from 192.168.20.22: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.20.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.20.21

Pinging 192.168.20.21 with 32 bytes of data:

Reply from 192.168.20.21: bytes=32 time<1ms TTL=128
Reply from 192.168.20.21: bytes=32 time<1ms TTL=128
Reply from 192.168.20.21: bytes=32 time<1ms TTL=128
Reply from 192.168.20.21: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.20.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Gambar 14 Hasil Test Koneksi Dari PC-RG2 ke PC-AK2 dan PC-RPL2



Gambar 15 Hasil Test Koneksi dari PC-RG3 ke PC-AK3 dan PC-RPL3

3.4 Pembahasan

Dalam lingkungan jaringan tanpa penggunaan Virtual LAN (VLAN), seluruh perangkat yang terhubung berada dalam satu *domain broadcast*, sehingga setiap *broadcast* yang dikirimkan oleh satu perangkat akan diterima oleh semua perangkat lain dalam jaringan. Kondisi ini menyebabkan tingginya lalu lintas *broadcast*, yang pada skala besar dapat menurunkan performa jaringan secara signifikan. Selain itu, tidak adanya segmentasi logis membuat perangkat dari berbagai departemen, seperti SW-Guru, SW-Ak dan SW-RPL, dapat saling berkomunikasi tanpa batasan, sehingga menimbulkan potensi risiko keamanan akibat tidak adanya isolasi lalu lintas antar kelompok pengguna.

Penerapan kebijakan akses yang spesifik berdasarkan fungsi atau departemen pun menjadi sulit dilakukan. Untuk menciptakan pemisahan jaringan dalam skenario tanpa VLAN, diperlukan infrastruktur fisik terpisah seperti penggunaan switch atau router tambahan, yang tentunya tidak efisien dan membutuhkan biaya lebih besar. Oleh karena itu, jaringan tanpa VLAN tidak mendukung fleksibilitas manajemen jaringan dan sangat tidak *scalable* untuk organisasi dengan jumlah perangkat yang besar, karena berpotensi menyebabkan kemacetan lalu lintas (*congestion*) dan kesulitan dalam pengelolaan jaringan secara keseluruhan.

Penerapan Virtual LAN (VLAN) terbukti memberikan dampak signifikan terhadap efisiensi, keamanan, dan skalabilitas jaringan, terutama dalam lingkungan organisasi dengan jumlah perangkat dan pengguna yang besar. Dengan VLAN, jaringan fisik yang sama dapat dipisahkan secara logis menjadi beberapa segmen yang berbeda berdasarkan fungsi, departemen, atau kebutuhan tertentu, seperti VLAN untuk guru, Lab Akutansi dan Lab RPL. Pemisahan ini menciptakan *domain broadcast* yang lebih kecil, sehingga *broadcast* dari suatu VLAN tidak akan menyebar ke VLAN lain, yang secara langsung mengurangi lalu lintas broadcast dan meningkatkan kinerja jaringan secara keseluruhan.

Dari sisi keamanan, VLAN memungkinkan isolasi lalu lintas antar grup pengguna, sehingga akses antar departemen dapat dikendalikan dan dibatasi sesuai dengan kebijakan organisasi. Selain itu, VLAN memberikan *fleksibilitas* tinggi dalam manajemen jaringan. *Administrator* dapat menambahkan, memindahkan, atau menghapus perangkat dari suatu VLAN tanpa harus mengubah koneksi fisik, cukup dengan mengkonfigurasi ulang *port* pada *switch*. Hal ini menghemat waktu, tenaga, dan biaya, serta memungkinkan pengelolaan jaringan yang lebih dinamis dan adaptif terhadap perubahan struktur organisasi. Penerapan VLAN juga membuat jaringan menjadi lebih scalable, karena penambahan perangkat atau pengembangan jaringan tidak mengakibatkan peningkatan *broadcast* secara menyeluruh. Dengan pembagian VLAN yang tepat, jaringan dapat tumbuh dengan lebih terstruktur dan terkendali.

4. KESIMPULAN

Berdasarkan hasil simulasi yang dilakukan diatas pada saat vlan belum didaftarkan, maka Seluruh perangkat berada dalam satu broadcast domain tidak ada pemisahan logis antar grup pengguna dan manajemen jaringan menjadi kurang fleksibel serta tidak optimal untuk skala besar. Dengan diterapkannya VLAN maka mengurangi *broadcast domain,* keamanan yang lebih baik, fleksibilitas dan kemudahan manajemen, segmentasi jaringan secara logis, skalabilitas lebih baik dan efisiensi penggunaan perangkat jaringan.

REFERENSI

[1] A. Fattah and D. Patriana, “Perancangan dan Implementasi Virtual Area Network pada Jaringan Universitas Balikpapan,” *JTE UNIBA*, vol. 7, no. 1, 2022.

[2] I. Wayan Bhaskara Budi Yoga and M. Agung Raharja, “Implementasi VLAN (Virtual Local Area Network) pada Rumah Sakit Mata Ramata,” *Elektronik Ilmu Komputer Udayana, Jurnal*, vol. 7, no. 3, pp. 2654–5101, 2019.

[3] A. Al-furqan Abra and A. Syarif Aziz, “Implementasi Access Control List (Acl) Dalam Perancangan Virtual Local Area Network Pada Smkn 1 Al-Mubarkeya,” 2025.

[4] M. Rahman and M. Dasuki, “Implementasi access control list (ACL) sebagai metode proteksi dan traffic control pada infrastruktur jaringan local area network (LAN),” *Jurnal Computer Science and Information Technology (CoSciTech)*, vol. 6, no. 1, pp. 68–76, 2025, doi: 10.37859/coscitech.v6i1.9102.

[5] 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 dan Informatika*, vol. 5, no. 2, pp. 225–260, 2023.
[6] S. Rosyidi *et al.*, "Analisis Dan Perancangan Jaringan Wireless Local Area Network Di SMP," 2022.
[7] D. R. Komilov and I. B. Tajibayev, "Improving The Use Of Virtual Lan (Vlan) Technology," *Web of Discoveries: Journal of Analysis and Inventions*, vol. 1, no. 7, pp. 6–11, 2023.
[8] A. Sopian *et al.*, "Perancangan Jaringan Virtual LAN Menggunakan Metode Protokol Peer-VLAN Spanning Tree Protokol Peer-Vlan Spanning Tree," *Jurnal Elektro & Informatika Swadharma (JEIS)*, vol. 02, no. 01, pp. 28–35, 2022.
[9] S. Sitohang and H. Pangaribuan, "Rancang Bangun Intrusion Detection System (Ids) Menggunakan Snort (Studi Kasus Pt Pln Batam)," *Jurnal Sistem Informasi & Manajemen (JURSIMA)*, vol. 11, no. 01, pp. 143–152, 2023.
[10] Silalahi; Putri Rosayanti and Sitohang; Sunarsan, "Analisis Keamanan Jaringan Pada Fasilitas Wifi Terhadap," *Jurnal Comasie*, vol. 9, no. 8, pp. 1031–1039, 2023.
[11] O. Efrén *et al.*, "Análisis de seguridad y contramedidas frente al VLAN Hopping Attack: evaluación y simulación en entornos de red," *Pro Sciences: Revista de Producción, Ciencias e Investigación*, vol. 8, no. 55, pp. 82–92, 2024, doi: 10.29018/issn.2588.
[12] T. Rahman, R. Zaini, G. Chrisnawati, K. Kunci, and : Vlan, "Perancangan Jaringan Virtual Local Area Network (Vlan) & Dhcp Pada Pt.Navicom Indonesia Bekasi," *Jurnal Teknik Informatika (JIKA) Universitas Muhammadiyah Tangerang*, pp. 36–41, 2020.
[13] Dedy Ariyadi and Sayekti Harits Suryawan, "Analisis dan Perancangan Jaringan Local Area Network Pada Labolatorium Komputer SMA Negeri 1 Long Iram," *SAFARI :Jurnal Pengabdian Masyarakat Indonesia*, vol. 4, no. 1, pp. 45–57, Dec. 2023, doi: 10.56910/safari.v4i1.1100.
[14] A. Prasetia Nanda, N. Aminudin, and M. Islamahdi, "Perancangan Arsitektur Jaringan Local Area Network Pada Smp Muhammadiyah 01 Pringsewu," *Aisyah Journal of Informatics and Electrical Engineering*, vol. 2, no. 2, pp. 120–125, 2020, [Online]. Available: http://jti.aisyahuniversity.ac.id/index.php/AJIEE
[15] S. Sitohang, H. Pangaribuan, and G. Sirait, "Pelatihan Virtual Local Area Network (Vlan) Dan Routing Di Sekolah Smk Tunas Muda Berkarya," *JUPADAI: Jurnal Pembinaan Kepada Masyarakat*, vol. 3, no. 2, pp. 56–63, 2024, [Online]. Available: https://jurnal-adaikepri.or.id/index.php/JUPADAI