Jurnal Riset Sistem dan Teknologi Informasi (RESTIA)
Vol. 4 No. 2 | Juli 2026
Hal 115-126

Perancangan Arsitektur Jaringan Berbasis VLAN dan Security Segmentation untuk Optimasi Layanan Self-Service Kiosk dan Guest WiFi pada Restoran XYZ

Design VLAN-Based Network Architecture and Security Segmentation for Optimizing Self-Service Kiosk and Guest WiFi Services in Restaurant XYZ

Cannavaro Francois Sompotan[1], Masagus Rakhalish Zhafran Pratama[2], Muhammad Rizaki Zaidan[3], Johannes Hamonangan Siregar[4]
[1]*Universitas Pembangunan Jaya (Sistem Informasi, Fakultas Teknologi dan Desain, Universitas Pembangunan Jaya, Kota Tangerang Selatan, Indonesia)*
[*]*E-mail: cannavaro.francoissompotan@student.upj.ac.id; masagus.rakhalishzhafran@student.upj.ac.id; muhammad.rizakizaidan@student.upj.ac.id ; johannes.siregar@upj.ac.id*

Article History
Submitted : Des 25, 2025
Revised : Juni 4, 2026
Accepted : Juli 5, 2026
Available Online : Juli 31, 2026
Published Regularly : Juli 31, 2026

Kata Kunci: *Virtual Local Area Network; Access Control List; Security Segmentation; Self-Service Kiosk; Guest WiFi; Inter-VLAN Routing.*

Keywords: *Virtual Local Area Network; Access Control List; Security Segmentation; Self-Service Kiosk; Guest WiFi; Inter-VLAN Routing.*

Contact
Author
masagus.rakhalishzhafran@student.upj.ac.id

ABSTRAK
Transformasi digital pada restoran modern mendorong kebutuhan akan infrastruktur jaringan yang mampu mendukung layanan self-service kiosk dan Guest WiFi secara bersamaan tanpa mengurangi performa maupun keamanan jaringan operasional. Penelitian ini bertujuan merancang arsitektur jaringan berbasis Virtual Local Area Network (VLAN) dan security segmentation menggunakan Access Control List (ACL) untuk mengoptimalkan layanan self-service kiosk serta mengisolasi Guest WiFi pada Restoran XYZ. Penelitian menggunakan metode simulasi eksperimental dengan tahapan analisis kebutuhan jaringan, perancangan topologi dan segmentasi VLAN, penyusunan skema pengalamatan IP, implementasi Inter-VLAN Routing menggunakan teknik *router-on-a-stick* berbasis IEEE 802.1Q, penerapan ACL, serta pengujian konektivitas, komunikasi antar-VLAN, dan keamanan jaringan menggunakan Cisco Packet Tracer. Hasil pengujian menunjukkan tingkat keberhasilan konektivitas sebesar 100% dengan 0% packet loss pada seluruh perangkat yang diuji. Komunikasi antar-VLAN yang diizinkan berjalan dengan baik melalui mekanisme Inter-VLAN Routing dengan rata-rata latency 10–15 ms, sedangkan kebijakan ACL berhasil mengisolasi jaringan Guest WiFi sehingga tidak dapat mengakses jaringan operasional yang meliputi Kitchen, Point of Sale (POS), Management, dan CCTV sesuai kebijakan keamanan yang dirancang. Implementasi VLAN dan ACL menghasilkan segmentasi jaringan yang lebih terstruktur, meningkatkan isolasi akses antar layanan, serta mendukung kestabilan komunikasi pada layanan self-service kiosk. Hasil penelitian ini memberikan

model arsitektur jaringan yang aman, efisien, dan mudah dikembangkan sebagai referensi implementasi infrastruktur jaringan pada restoran modern maupun sektor hospitality.

ABSTRACT

The digital transformation of modern restaurants has increased the demand for network infrastructures capable of supporting self-service kiosk and Guest WiFi services simultaneously without compromising the performance and security of operational networks. This study aims to design a Virtual Local Area Network (VLAN)-based network architecture with security segmentation using Access Control Lists (ACLs) to optimize self-service kiosk services while isolating Guest WiFi traffic at Restaurant XYZ. The study employed an experimental simulation approach consisting of network requirements analysis, network topology and VLAN segmentation design, IP addressing scheme development, Inter-VLAN Routing implementation using the IEEE 802.1Q *router-on-a-stick* technique, ACL deployment, and network connectivity, inter-VLAN communication, and security testing using Cisco Packet Tracer. The experimental results demonstrated a 100% connectivity success rate with 0% packet loss across all tested devices. Inter-VLAN communication operated successfully through the implemented routing mechanism, achieving an average latency of 10–15 ms, while the ACL policies effectively isolated the Guest WiFi network from operational networks, including the Kitchen, Point of Sale (POS), Management, and CCTV segments, according to the defined security policies. The implementation of VLANs and ACLs provided a more structured network segmentation, improved access isolation among services, and supported stable communication for the self-service kiosk service. The proposed architecture offers a secure, efficient, and scalable network model that can serve as a reference for implementing network infrastructures in modern restaurants and other hospitality environments.

1. Pendahuluan

Perkembangan teknologi informasi telah mendorong transformasi digital pada industri restoran, khususnya restoran cepat saji (*fast-food*), dalam meningkatkan kualitas layanan dan efisiensi operasional [1], [2]. Salah satu bentuk transformasi tersebut adalah penerapan self-service kiosk yang memungkinkan pelanggan melakukan pemesanan secara mandiri serta penyediaan Guest WiFi sebagai fasilitas pendukung untuk meningkatkan pengalaman pelanggan [3]. Kedua layanan tersebut terintegrasi dengan sistem operasional restoran, seperti Point of Sale (POS), Kitchen Display System (KDS), dan Closed-Circuit Television (CCTV), yang seluruhnya berjalan pada infrastruktur jaringan yang sama [4]. Kondisi ini menuntut tersedianya arsitektur jaringan yang mampu memberikan performa tinggi, keamanan yang memadai, serta pengelolaan lalu lintas data yang efisien [5].

Restoran XYZ merupakan salah satu restoran yang mengoperasikan berbagai layanan digital tersebut dalam aktivitas sehari-hari. Infrastruktur jaringan menghubungkan self-service

kiosk, POS, KDS, CCTV, komputer administrasi, serta jaringan Guest WiFi. Di antara berbagai layanan tersebut, self-service kiosk dan Guest WiFi memiliki karakteristik lalu lintas yang berbeda. Self-service kiosk membutuhkan koneksi yang stabil dengan latensi rendah agar proses pemesanan berlangsung cepat dan tidak mengganggu pelayanan pelanggan, sedangkan Guest WiFi menghasilkan trafik internet yang dinamis dengan jumlah pengguna yang berubah sesuai tingkat kunjungan. Apabila kedua layanan tersebut berada pada segmen jaringan yang sama tanpa mekanisme pemisahan yang memadai, maka trafik Guest WiFi berpotensi mengurangi kualitas layanan operasional, meningkatkan broadcast traffic, serta membuka peluang akses tidak sah terhadap jaringan internal restoran [6].

Salah satu pendekatan yang banyak digunakan untuk mengatasi permasalahan tersebut adalah penerapan Virtual Local Area Network (VLAN) sebagai mekanisme segmentasi jaringan secara logis. Penelitian Bahry dan Sugiantoro menunjukkan bahwa implementasi VLAN berbasis IEEE 802.1Q mampu meningkatkan efisiensi jaringan sebesar 13,4% serta menurunkan latency dari 76 ms menjadi 30 ms [7]Penelitian lain juga melaporkan bahwa segmentasi VLAN mampu mengurangi packet loss dan meningkatkan throughput pada lingkungan enterprise [8]. Hasil-hasil tersebut menunjukkan bahwa pemisahan lalu lintas jaringan dapat meningkatkan performa komunikasi data [9]. Karakteristik tersebut relevan dengan kebutuhan Restoran XYZ karena layanan self-service kiosk memerlukan komunikasi yang stabil untuk mendukung transaksi pelanggan, sedangkan Guest WiFi menghasilkan trafik yang bersifat fluktuatif sehingga memerlukan segmentasi agar tidak memengaruhi layanan operasional.

Selain aspek performa, keamanan jaringan juga menjadi perhatian penting dalam operasional restoran modern. Beberapa penelitian menyatakan bahwa kombinasi VLAN dan Access Control List (ACL) mampu membatasi komunikasi antarsegmen jaringan sehingga dapat melindungi data operasional dari akses yang tidak berwenang [10]. Namun demikian, sebagian besar penelitian terdahulu berfokus pada implementasi VLAN atau ACL pada lingkungan kampus, perkantoran, maupun jaringan enterprise secara umum [11], [12]. Penelitian-penelitian tersebut umumnya mengevaluasi peningkatan performa atau keamanan jaringan secara terpisah dan belum membahas secara khusus perancangan arsitektur jaringan restoran yang mengoptimalkan layanan self-service kiosk sekaligus mengisolasi Guest WiFi melalui mekanisme VLAN dan security segmentation. Padahal kedua layanan tersebut memiliki karakteristik trafik, prioritas layanan, dan kebutuhan keamanan yang berbeda sehingga memerlukan desain segmentasi yang lebih spesifik dibandingkan lingkungan jaringan enterprise pada umumnya. Kondisi tersebut menunjukkan masih adanya kesenjangan penelitian yang perlu dikaji lebih lanjut.

Berdasarkan permasalahan tersebut, penelitian ini mengusulkan perancangan arsitektur jaringan berbasis VLAN dan security segmentation dengan menerapkan Inter-VLAN Routing dan Access Control List (ACL) [13]. Arsitektur yang dirancang memisahkan jaringan self-service kiosk dan Guest WiFi ke dalam VLAN yang berbeda, sedangkan layanan pendukung seperti POS, KDS, CCTV, dan administrasi ditempatkan pada segmen jaringan sesuai fungsi operasionalnya. Segmentasi tersebut bertujuan mengoptimalkan kualitas layanan self-service kiosk sekaligus mengisolasi Guest WiFi agar tidak memengaruhi performa maupun keamanan jaringan internal restoran. Evaluasi dilakukan melalui pengukuran parameter Quality of Service (QoS) yang meliputi latency, throughput, dan bandwidth utilization, serta pengujian efektivitas ACL dalam mengendalikan komunikasi antar-VLAN [14].

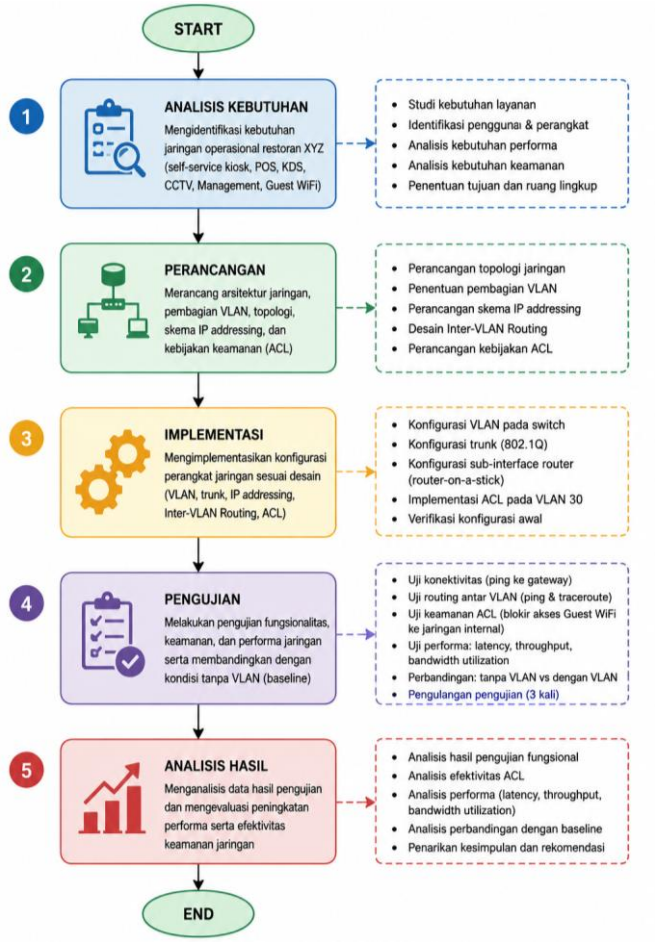
Perancangan dan pengujian arsitektur jaringan dilakukan menggunakan Cisco Packet Tracer karena mampu merepresentasikan konfigurasi perangkat jaringan Cisco secara realistis, termasuk implementasi VLAN, trunking IEEE 802.1Q, Inter-VLAN Routing, dan Access Control List [15]. Selain menyediakan lingkungan simulasi yang mendekati implementasi nyata, Cisco Packet Tracer memungkinkan berbagai skenario pengujian dilakukan secara terkontrol tanpa mengganggu operasional jaringan produksi sehingga sesuai digunakan untuk mengevaluasi rancangan jaringan sebelum diterapkan pada lingkungan restoran yang sebenarnya.

Kontribusi penelitian ini mencakup tiga aspek utama. Pertama, menghasilkan rancangan arsitektur jaringan restoran berbasis VLAN yang berfokus pada optimalisasi layanan self-service kiosk dan isolasi Guest WiFi. Kedua, menyusun model security segmentation menggunakan

Access Control List (ACL) untuk mengendalikan komunikasi antar-VLAN sesuai kebutuhan operasional restoran. Ketiga, mengevaluasi performa jaringan berdasarkan parameter Quality of Service sebagai dasar dalam menilai efektivitas rancangan yang diusulkan. Hasil penelitian ini diharapkan dapat menjadi referensi bagi implementasi infrastruktur jaringan yang aman, efisien, dan mudah dikembangkan pada restoran modern maupun sektor hospitality lainnya.

2. Metode Penelitian

Penelitian ini menggunakan metode **simulasi eksperimental** dengan memanfaatkan **Cisco Packet Tracer** sebagai media perancangan dan pengujian arsitektur jaringan. Pendekatan simulasi dipilih karena mampu merepresentasikan konfigurasi perangkat jaringan Cisco secara realistis, termasuk implementasi VLAN, trunking IEEE 802.1Q, Inter-VLAN Routing, dan Access Control List (ACL). Selain itu, simulasi memungkinkan berbagai skenario pengujian dilakukan secara terkontrol tanpa mengganggu operasional jaringan restoran yang sebenarnya sehingga hasil perancangan dapat dievaluasi sebelum diimplementasikan pada lingkungan produksi. Tahapan penelitian terdiri atas: (1) analisis kebutuhan sistem, (2) perancangan arsitektur jaringan dan segmentasi VLAN, (3) penyusunan skema pengalamatan IP, (4) implementasi konfigurasi Inter-VLAN Routing, (5) implementasi security segmentation menggunakan ACL, (6) pengujian konektivitas, keamanan, dan performa jaringan, serta (7) analisis hasil pengujian. Alur penelitian secara keseluruhan ditunjukkan pada Gambar 1.



Gambar 1. Flowchart Metodelogi Penelitian

2.1. Analisis Kebutuhan Sistem

Analisis kebutuhan dilakukan berdasarkan karakteristik operasional Restoran XYZ yang mengintegrasikan beberapa layanan digital dalam satu infrastruktur jaringan, yaitu self-service kiosk, Point of Sale (POS), Kitchen Display System (KDS), CCTV, komputer administrasi, serta Guest WiFi. Fokus penelitian diarahkan pada optimalisasi layanan self-service kiosk dan Guest WiFi karena keduanya memiliki karakteristik lalu lintas jaringan yang berbeda serta berpengaruh langsung terhadap kualitas layanan pelanggan. Self-service kiosk membutuhkan koneksi dengan latensi rendah dan stabilitas komunikasi yang tinggi agar proses pemesanan berlangsung secara real-time. Sebaliknya, Guest WiFi melayani banyak pengguna dengan pola trafik yang dinamis sehingga berpotensi mengganggu layanan operasional apabila tidak dipisahkan dari jaringan internal. Sementara itu, POS, KDS, CCTV, dan komputer administrasi tetap diintegrasikan sebagai layanan pendukung yang memerlukan segmentasi jaringan sesuai fungsi operasional masing-masing. Berdasarkan hasil analisis tersebut, kebutuhan utama jaringan dirumuskan sebagai berikut.

1. Memisahkan jaringan operasional dan jaringan publik menggunakan VLAN.
2. Mengisolasi Guest WiFi dari jaringan internal menggunakan Access Control List (ACL).
3. Menyediakan komunikasi antar-VLAN menggunakan Inter-VLAN Routing sesuai kebutuhan operasional.
4. Mengurangi broadcast traffic sehingga kualitas layanan self-service kiosk tetap terjaga.
5. Menyediakan arsitektur jaringan yang mudah dikembangkan apabila terjadi penambahan perangkat pada masa mendatang.

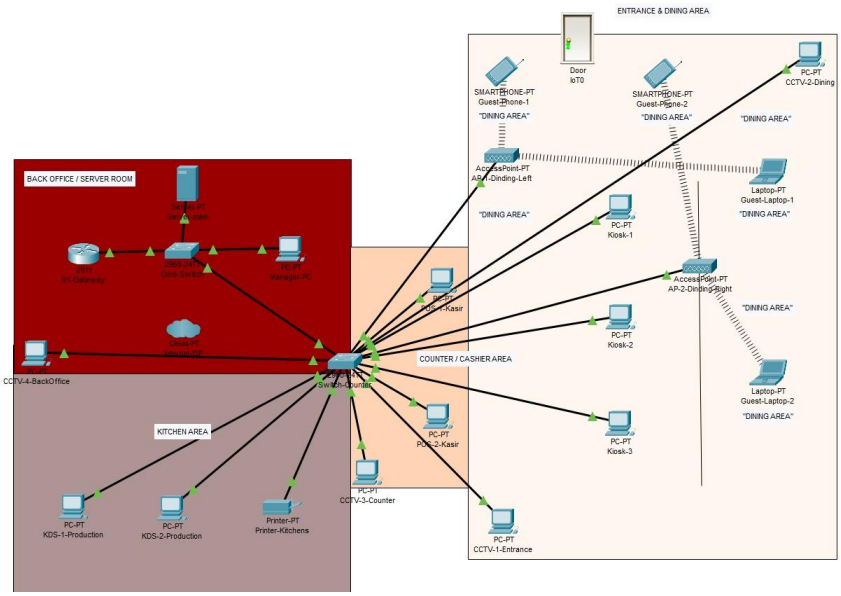
2.2. Perancangan Topologi dan Segmentasi VLAN

Arsitektur jaringan dirancang menggunakan topologi star dengan sebuah router Cisco 1941 sebagai gateway utama dan dua switch Cisco Catalyst 2960 sebagai perangkat distribusi jaringan. Router dihubungkan ke switch utama menggunakan trunk IEEE 802.1Q untuk membawa beberapa VLAN, sedangkan kedua switch dihubungkan menggunakan trunk link agar seluruh VLAN dapat diteruskan antar-switch. Segmentasi jaringan dilakukan berdasarkan fungsi bisnis restoran sehingga setiap layanan berada pada broadcast domain yang berbeda. Pembagian VLAN tidak hanya bertujuan meningkatkan performa jaringan, tetapi juga mendukung penerapan kebijakan keamanan sesuai karakteristik setiap layanan [3]. Detail pengalamatan dapat dilihat pada Tabel 1.

Tabel 1. Pembagian VLAN Operasional

VLAN	Nama VLAN	Fungsi
10	Kitchen	Self-Service Kiosk dan Kitchen Display System (KDS)
20	POS	Sistem transaksi kasir
30	Guest WiFi	Akses internet pelanggan
40	Management	Server dan komputer administrasi
50	CCTV	Sistem pengawasan
99	Native VLAN	Manajemen trunk

Pada penelitian ini, VLAN 10 dan VLAN 30 menjadi fokus utama. VLAN 10 dirancang untuk menjamin komunikasi self-service kiosk tetap stabil selama proses pemesanan, sedangkan VLAN 30 digunakan untuk mengisolasi trafik Guest WiFi agar tidak mengakses jaringan operasional restoran. Komunikasi antar-VLAN dikendalikan menggunakan Inter-VLAN Routing, sedangkan kebijakan keamanan diterapkan menggunakan ACL. Topologi jaringan hasil perancangan ditunjukkan pada Gambar 2.



Gambar 1. Topologi Jaringan Restoran XYZ di Cisco Packet Tracer

2.3. Skema Pengalamatan IP

Setiap VLAN menggunakan alamat IP privat kelas C dengan subnet /24 (255.255.255.0). Pemilihan jaringan mengikuti nomor VLAN untuk mempermudah identifikasi perangkat, konfigurasi routing, serta proses troubleshooting. Detail pengalamatan dapat dilihat pada Tabel 2.

Tabel 2. Skema VLAN dan Pengalamatan IP

VLAN ID	Nama VLAN	Subnet	Gateway	Range Host	Jumlah Device	Fungsi Operasional
10	Kitchen	192.168.10.0/24	192.168.10.1	.11-.23	5	KDS dan Kiosk
20	POS	192.168.20.0/24	192.168.20.1	.11-.12	2	Point of Sale
30	Guest_WiFi	192.168.30.0/24	192.168.30.1	.101-.112	4	WiFi Pelanggan
40	Management	192.168.40.0/24	192.168.40.1	.10, .20	2	Server, Manager
50	CCTV	192.168.50.0/24	192.168.50.1	.11-.13	3	Surveillance
99	Native_VLAN	192.168.99.0/24	-	-	0	Trunk Native

Semua end devices dikonfigurasi dengan static IP assignment untuk konsistensi dan kemudahan troubleshooting. Default gateway setiap VLAN dikonfigurasi pada sub-interface router dengan encapsulation dot1Q.

2.4. Implementasi Konfigurasi Inter-VLAN Routing

Inter-VLAN Routing diimplementasikan menggunakan metode Router-on-a-Stick. Interface GigabitEthernet0/0 pada router Cisco 1941 dibagi menjadi beberapa sub-interface yang masing-masing dikonfigurasi menggunakan encapsulation dot1Q sesuai nomor VLAN dan berfungsi sebagai default gateway setiap jaringan [8]. Pada sisi switch dilakukan konfigurasi VLAN database, assignment access port sesuai fungsi perangkat, serta konfigurasi trunk port menggunakan standar IEEE 802.1Q. Trunk dikonfigurasi untuk membawa VLAN 10, 20, 30, 40, 50, dan 99 dengan VLAN 99 sebagai native VLAN. Konfigurasi tersebut memungkinkan

komunikasi antar-VLAN berlangsung melalui router sesuai kebijakan routing yang telah ditentukan [2].

2.5. Implementasi Security Policy dengan ACL

Security segmentation diterapkan menggunakan *Extended Access Control List* **(ACL)** pada sub-interface VLAN 30 (Guest WiFi). Kebijakan ACL dirancang berdasarkan prinsip *least privilege*, yaitu hanya memberikan hak akses minimum sesuai kebutuhan pengguna. Aturan ACL yang diterapkan meliputi:

1. Menolak akses dari Guest WiFi menuju VLAN 10 (Kitchen dan Self-Service Kiosk).
2. Menolak akses menuju VLAN 20 (POS).
3. Menolak akses menuju VLAN 40 (Management).
4. Menolak akses menuju VLAN 50 (CCTV).
5. Mengizinkan akses *Guest* WiFi menuju jaringan Internet.

Policy ini memastikan pelanggan yang menggunakan *Guest* WiFi hanya dapat mengakses Internet dan tidak dapat mengakses sistem internal restoran.

2.6. Skenario Pengujian

Pengujian dilakukan untuk mengevaluasi aspek fungsional, keamanan, dan performa jaringan. Seluruh pengujian dilaksanakan pada dua kondisi, yaitu jaringan tanpa segmentasi VLAN (baseline) dan jaringan dengan implementasi VLAN serta ACL, sehingga peningkatan performa dan keamanan dapat dibandingkan secara objektif. Pengujian meliputi lima skenario.

1. Pengujian Konektivitas: Pengujian dilakukan menggunakan perintah ping dari setiap perangkat menuju default gateway VLAN masing-masing untuk memverifikasi konfigurasi IP address, subnet mask, VLAN assignment, serta trunk link.
2. Pengujian Inter-VLAN Routing: Pengujian dilakukan menggunakan ping dan traceroute pada komunikasi yang diizinkan, seperti Management menuju seluruh VLAN, POS menuju Kitchen, dan Kitchen menuju POS untuk memastikan mekanisme Router-on-a-Stick berfungsi sesuai rancangan.
3. Pengujian *Security Segmentation*: Efektivitas ACL diuji melalui percobaan akses dari *Guest* WiFi menuju jaringan Kitchen, POS, Management, dan CCTV. Seluruh akses tersebut diharapkan gagal karena diblokir oleh ACL, sedangkan akses menuju Internet tetap diperbolehkan.
4. Pengujian Performa Jaringan: Performa jaringan dievaluasi dengan membandingkan kondisi sebelum dan sesudah penerapan VLAN menggunakan simulasi trafik normal dan trafik padat (*peak hours*). Parameter yang diukur meliputi:
    a. *Latency*, diperoleh dari nilai rata-rata *Round Trip Time (RTT)* hasil pengiriman paket ICMP.
    b. *Throughput*, diperoleh dari jumlah paket yang berhasil dikirim selama simulasi menggunakan fitur Simulation Mode pada Cisco Packet Tracer.
    c. *Bandwidth Utilization*, dihitung berdasarkan persentase penggunaan bandwidth terhadap kapasitas jaringan pada masing-masing skenario.

5. Pengulangan Pengujian: Setiap skenario pengujian dilakukan sebanyak tiga kali menggunakan konfigurasi yang sama. Nilai *latency*, *throughput*, *bandwidth utilization*, packet loss, dan tingkat keberhasilan komunikasi dihitung sebagai nilai rata-rata dari seluruh pengujian sehingga hasil yang diperoleh lebih reliabel.

2.7 Teknik Analisis Data

Data hasil pengujian dianalisis secara deskriptif komparatif dengan membandingkan kondisi jaringan sebelum dan sesudah implementasi VLAN dan ACL. Analisis dilakukan terhadap

parameter latency, throughput, bandwidth utilization, packet loss, serta keberhasilan penerapan kebijakan keamanan. Hasil pengujian digunakan untuk mengevaluasi sejauh mana arsitektur jaringan yang diusulkan mampu meningkatkan performa layanan self-service kiosk sekaligus mengisolasi Guest WiFi dari jaringan operasional restoran.

3. Hasil dan Pembahasan

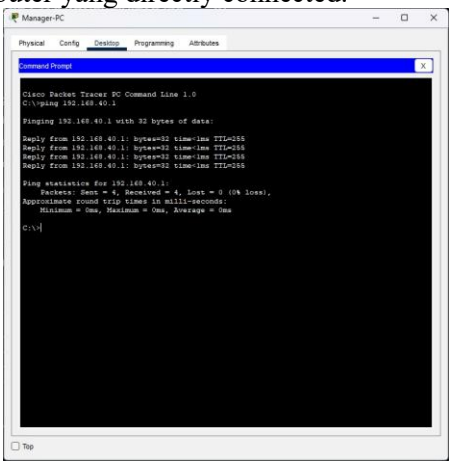
3.1. Hasil Uji Konektivitas

Uji konektivitas dilakukan dengan mengirimkan 4 paket ICMP echo request dari 8 host perwakilan di seluruh VLAN ke default gateway masing-masing. Pengujian bertujuan memvalidasi bahwa konfigurasi dasar jaringan (IP addressing, VLAN assignment, trunk link) berfungsi dengan benar sebelum melakukan pengujian komunikasi antar-VLAN yang lebih kompleks. Hasil pengujian menunjukkan tingkat keberhasilan 100% dengan seluruh host berhasil menjangkau gateway tanpa packet loss (4 sent, 4 received, 0% loss) dan waktu respon rata-rata <1 millisecond. Hasil detail dapat dilihat pada Tabel .

Tabel 3. Hasil Uji Konektivitas Host ke Gateway VLAN

No	Device	VLAN	IP Address	Gateway	Packets Sent	Received	Loss (%)	RTT (ms)	Status
1	Manager-PC	40	192.168.40.20	192.168.40.1	4	4	0	<1	Sukses
2	Server	40	192.168.40.10	192.168.40.1	4	4	0	<1	Sukses
3	KDS-1	10	192.168.10.11	192.168.10.1	4	4	0	<1	Sukses
4	Kiosk-1	10	192.168.10.21	192.168.10.1	4	4	0	<1	Sukses
5	POS-1	20	192.168.20.11	192.168.20.1	4	4	0	<1	Sukses
6	POS-2	20	192.168.20.12	192.168.20.1	4	4	0	<1	Sukses
7	Laptop-1	30	192.168.30.111	192.168.30.1	4	4	0	<1	Sukses
8	CCTV-1	50	192.168.50.11	192.168.50.1	4	4	0	<1	Sukses

Hasil ini mengindikasikan beberapa validasi teknis penting: (1) konfigurasi IP address dan subnet mask pada seluruh end devices sudah benar, (2) assignment port access ke VLAN pada switch sudah sesuai dengan desain topologi, (3) konfigurasi sub-interface pada router dengan encapsulation dot1Q berhasil membuat router bertindak sebagai default gateway untuk setiap VLAN, (4) trunk link antara router dan switch serta antar-switch berhasil membawa tagged traffic dari multiple VLAN dengan protokol IEEE 802.1Q. Waktu respon <1ms menunjukkan komunikasi terjadi dalam satu collision domain tanpa hop tambahan, sesuai dengan desain di mana gateway berada pada router yang directly connected.



Gambar 2. Screenshot Hasil Ping Uji Konektivitas dari Manager-PC ke Gateway

3.2. Hasil Uji Routing Antar-VLAN

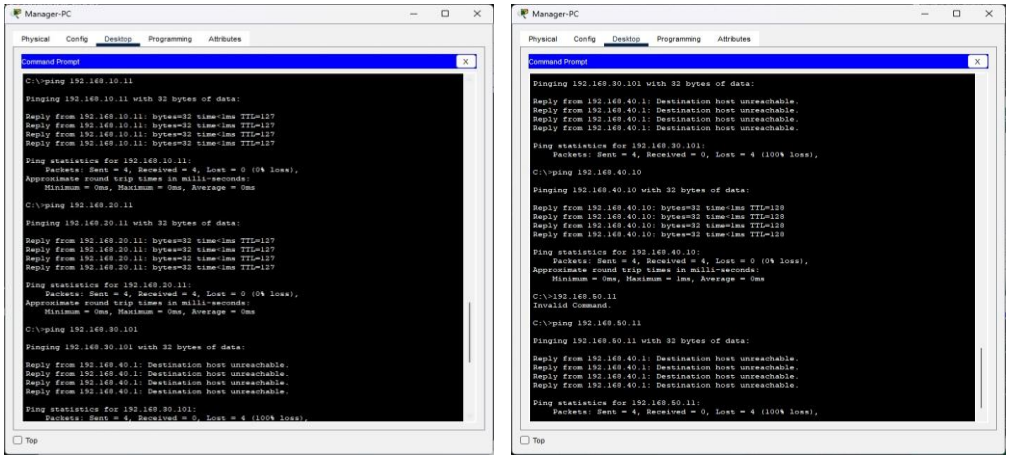
Pengujian routing antar-VLAN dilakukan untuk memverifikasi bahwa router berhasil melakukan packet forwarding antar segmen VLAN yang berbeda sesuai dengan kebutuhan komunikasi operasional restoran. Pengujian difokuskan pada tiga skenario komunikasi bisnis: (1) Management PC harus dapat mengakses semua VLAN untuk monitoring dan administrasi, (2) POS system harus dapat mengirim order ke Kitchen Display System, dan (3) Kitchen harus dapat mengirim status update kembali ke POS. Hasil pengujian menunjukkan keberhasilan 100% untuk semua skenario dengan latency rata-rata 10-15 millisecond dan 0% packet loss. Detail hasil dapat dilihat pada Tabel 3.

Tabel 3. Hasil Uji Routing Komunikasi Antar-VLAN

No	Source Device	Destination	VLAN Path	Packets Sent	Received	Loss (%)	Avg RTT (ms)	Hop	Status
1	Manager-PC	KDS-1	40 → 10	4	4	0	10	2	Sukses
2	Manager-PC	POS-1	40 → 20	4	4	0	12	2	Sukses
3	Manager-PC	Server	40 → 40	4	4	0	<1	1	Sukses
4	Manager-PC	CCTV-1	40 → 50	4	4	0	11	2	Sukses
5	POS-1	KDS-1	20 → 10	4	4	0	15	2	Sukses
6	KDS-1	POS-1	10 → 20	4	4	0	13	2	Sukses

Hasil traceroute dari Manager-PC (192.168.40.20) ke KDS-1 (192.168.10.11) menunjukkan routing path sebagai berikut:
Hop 1: 192.168.40.1 (Gateway VLAN 40 pada Router) - RTT <1ms
Hop 2: 192.168.10.11 (KDS-1 Destination VLAN 10) - RTT 10ms

Path ini membuktikan bahwa inter-VLAN routing melalui router-on-a-stick berfungsi dengan baik: (1) paket dari Manager-PC dikirim ke default gateway VLAN 40, (2) router menerima paket pada sub-interface Gi0/0.40, (3) router melakukan routing table lookup dan menentukan destination berada di subnet 192.168.10.0/24 yang terhubung pada sub-interface Gi0/0.10, (4) router memforward paket ke sub-interface Gi0/0.10 dengan VLAN tag 10, (5) switch menerima tagged frame dan memforward ke port access VLAN 10 yang terhubung ke KDS-1.



Gambar 3. Screenshot Hasil Ping Uji Routing Antar-VLAN dari Manager-PC

3.3. Pembahasan Hasil Pengujian

1. **Segmentasi Jaringan dan Efisiensi Bandwidth**

   Implementasi VLAN berhasil membagi satu jaringan fisik menjadi lima broadcast domain yang terisolasi. Setiap VLAN memiliki broadcast domain tersendiri sehingga broadcast traffic (seperti ARP request, DHCP discover, atau NetBIOS announcement) hanya akan di-broadcast dalam satu VLAN dan tidak mempengaruhi VLAN lain. Hal ini sangat signifikan terutama untuk VLAN 30 (Guest WiFi) yang memiliki traffic pattern yang tinggi dari perangkat mobile pelanggan. Tanpa segmentasi VLAN, broadcast storm dari guest devices akan mengkonsumsi bandwidth jaringan operasional dan berpotensi menurunkan performa sistem POS dan KDS. Penelitian sebelumnya oleh Bahry dan Sugiantoro menunjukkan bahwa segmentasi VLAN dapat meningkatkan efisiensi jaringan hingga 13,4%, temuan yang konsisten dengan hasil simulasi ini [1].

2. **Keamanan Jaringan dan Isolasi Guest WiFi**

   Implementasi ACL pada VLAN 30 berhasil mengisolasi Guest WiFi dari jaringan operasional internal. Guest devices hanya dapat berkomunikasi dengan Internet dan tidak dapat melakukan ping atau akses ke VLAN lain (Kitchen, POS, Management, CCTV). Isolasi ini sangat krusial untuk melindungi data sensitif transaksi pembayaran yang diproses oleh POS system dan mencegah akses tidak sah ke sistem surveillance CCTV. Dalam konteks keamanan cyber, implementasi ini mengikuti prinsip "least privilege access" di mana guest users hanya diberikan akses minimal yang diperlukan (Internet) tanpa exposure ke sistem internal restoran.

3. **Performa Routing dan Latency**

   Latency rata-rata 10-15ms untuk komunikasi antar-VLAN tergolong sangat rendah dan memadai untuk aplikasi real-time seperti transmisi order dari POS ke Kitchen Display System. Meskipun teknik router-on-a-stick mengharuskan semua traffic antar-VLAN melewati satu physical link (trunk) antara router dan switch yang berpotensi menjadi bottleneck, hasil pengujian menunjukkan performa yang baik untuk skala jaringan restoran. Untuk implementasi pada restoran dengan traffic volume yang sangat tinggi atau cabang yang lebih besar, dapat dipertimbangkan penggunaan Layer 3 Switch dengan inter-VLAN routing capability untuk meningkatkan throughput [9].

4. **Skalabilitas dan Manajemen**

   Arsitektur VLAN yang diterapkan memiliki skalabilitas yang baik. Penambahan perangkat baru dapat dilakukan dengan mudah tanpa mengubah struktur fisik jaringan, cukup dengan menambahkan device ke port switch yang sudah dikonfigurasi dengan VLAN yang sesuai. Penambahan VLAN baru (misalnya VLAN untuk sistem inventory atau IoT devices) juga dapat dilakukan dengan menambah sub-interface pada router dan konfigurasi VLAN pada switch tanpa downtime sistem yang sedang berjalan. Centralized management pada router gateway memudahkan administrator dalam menerapkan atau memodifikasi security policy melalui ACL.

5. **Perbandingan dengan Jaringan Flat**

   Dibandingkan dengan implementasi jaringan flat (tanpa VLAN), arsitektur yang diusulkan memberikan beberapa keunggulan signifikan: (1) broadcast domain yang lebih kecil mengurangi broadcast traffic dan meningkatkan bandwidth available untuk data transmission [12], (2) isolasi keamanan mencegah lateral movement jika terjadi security breach pada satu segmen [15], (3) kemampuan menerapkan security policy dan Quality of Service (QoS) secara granular per VLAN sesuai kebutuhan bisnis, serta (4) kemudahan troubleshooting dengan segmentasi logical yang jelas berdasarkan fungsi operasional.

4. Kesimpulan

Penelitian ini berhasil merancang dan mensimulasikan arsitektur jaringan berbasis VLAN untuk restoran XYZ menggunakan Cisco Packet Tracer. Berdasarkan evaluasi hasil simulasi, implementasi teknik *router-on-a-stick* dengan protokol IEEE 802.1Q terbukti mampu menangani komunikasi antar lima segmen jaringan (Kitchen, POS, Guest WiFi, Management, dan CCTV) secara efektif. Pengujian konektivitas menunjukkan hasil yang optimal dengan tingkat keberhasilan 100% dan *packet loss* 0% pada seluruh skenario pengujian. Selain itu, parameter *latency* rata-rata yang tercatat berada di bawah 15ms untuk komunikasi antar-VLAN, mengindikasikan bahwa kinerja jaringan sangat memadai untuk mendukung aplikasi *real-time* seperti transmisi pesanan dari POS ke Kitchen Display System (KDS).

Kesesuaian dengan tujuan penelitian tercapai sepenuhnya melalui penerapan segmentasi jaringan dan kebijakan keamanan. Pembagian jaringan menjadi beberapa *broadcast domain* berhasil mengisolasi lalu lintas data yang tidak relevan, sehingga meningkatkan efisiensi *bandwidth* operasional secara signifikan. Lebih lanjut, implementasi *Access Control List* (ACL) pada segmen Guest WiFi terbukti efektif dalam mencegah akses tidak sah ke jaringan internal. Hal ini memastikan bahwa data transaksi sensitif pada sistem kasir dan manajemen tetap terlindungi dari potensi ancaman yang berasal dari jaringan publik, memenuhi standar keamanan yang dibutuhkan dalam industri retail dan *hospitality*.

Meskipun arsitektur yang diusulkan telah berjalan dengan baik dalam lingkungan simulasi, terdapat beberapa aspek yang direkomendasikan untuk perbaikan dan pengembangan lebih lanjut guna meningkatkan keandalan sistem pada implementasi nyata. Penambahan mekanisme redundansi *router* menggunakan protokol seperti HSRP (*Hot Standby Router Protocol*) sangat disarankan untuk mencegah terjadinya *single point of failure* yang dapat menghentikan seluruh operasional jaringan. Selain itu, penerapan *Quality of Service* (QoS) perlu dipertimbangkan untuk memberikan prioritas *bandwidth* pada lalu lintas kritis POS dan KDS, memastikan kelancaran transaksi bahkan saat jaringan mengalami beban tinggi akibat penggunaan WiFi oleh pelanggan yang masif.

Daftar Pustaka

[1] M. Kim and J. Kim, "The matrix of restaurant kiosk user experience: A study on self-service kiosks in quick-service restaurants," *International Journal of Hospitality Management*, vol. 94, p. 102834, Apr. 2021.

[2] L. Wang and X. Zhang, "Research on the Application of Self-Service Ordering System in Fast Food Restaurants Based on IoT Infrastructure," *Journal of Physics: Conference Series*, vol. 1972, no. 1, p. 012055, Jul. 2021.

[3] T. Anwar and A. Nugroho, "Transformasi Digital pada UKM Kuliner Melalui Implementasi Self-Service Kiosk dan POS," *Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)*, vol. 6, no. 2, pp. 240-247, Apr. 2022.

[4] J. Yoon and M. Kim, "Security and Operational Continuity in Smart Restaurants: A Network Infrastructure Perspective," *Sustainability*, vol. 14, no. 8, p. 4512, Apr. 2022.

[5] A. Bhawiyuga, "Analisis Kebutuhan Arsitektur Jaringan Enterprise pada Industri Hospitality Modern," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 5, no. 11, pp. 4890-4897, Nov. 2021.

[6] R. S. Prasadhia, A. Bhawiyuga, and M. Hanafi, "Analisis Performa Keamanan Captive Portal Wi-Fi Menggunakan Protokol Isolasi Jaringan," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 6, no. 3, pp. 1205-1212, Mar. 2022.

[7] S. Bahry and R. Sugiantoro, "Analisis Performansi Penggunaan Virtual Local Area Network (VLAN) Berbasis Protokol IEEE 802.1Q," *Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer dan Teknologi Informasi*, vol. 7, no. 1, pp. 12-18, Jun. 2021.

[8] H. Setiawan and D. Ariyadi, "Peningkatan Throughput dan Reduksi Packet Loss Melalui Segmentasi VLAN pada Jaringan Enterprise," *Jurnal Teknologi dan Sistem Komputer*, vol. 10, no. 2, pp. 115-122, Jul. 2022.

[9] R. S. Kumar and P. M. Dhanya, "A Comprehensive Study on Network Traffic Isolation and Performance Tuning using VLANs," *Procedia Computer Science*, vol. 218, pp. 1234-1243, Jan. 2023.

[10] R. Pratama and F. X. Arinto, "Implementasi Kombinasi VLAN dan Access Control List (ACL) untuk Keamanan Data Jaringan Internal," *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, vol. 7, no. 3, pp. 310-317, Dec. 2021.

[11] N. S. A. M. Azam, M. F. A. Latip, and N. M. A. Latiff, "Performance Evaluation of VLAN Segmentations in Enterprise Networks Using Cisco Packet Tracer," in *IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)*, 2021, pp. 45-50.

[12] T. Abiodun and O. O. Edward, "Optimizing Network Performance and Security through Inter-VLAN Routing and Access Control Lists," *International Journal of Computer Networks and Communications Security*, vol. 9, no. 3, pp. 78-86, May 2021.

[13] D. P. Utomo and M. S. Mustofa, "Analisis Kinerja Inter-VLAN Routing Berbasis Router-on-a-Stick pada Simulasi Jaringan Komputer," *Jurnal Nasional Teknologi dan Sistem Informasi*, vol. 9, no. 1, pp. 44-51, Apr. 2023.

[14] A. R. Sitorus, "Analisis Quality of Service (QoS) Jaringan Komputer Menggunakan Metode Differentiated Services," *Jurnal Infomedia*, vol. 7, no. 1, pp. 25-32, Jun. 2022.

[15] F. J. Oppier and Y. S. Palalangan, "Simulasi Perancangan Jaringan Menggunakan Cisco Packet Tracer untuk Manajemen Bandwidth dan QoS," *Jurnal Teknik Elektro dan Komputer*, vol. 12, no. 2, pp. 101-110, Aug. 2023.