

Perancangan Jaringan IoT Smart Home dengan Segmentasi VLAN untuk Mendukung Otomasi dan Keamanan Sistem

Design IoT-Based Smart Home Network Using VLAN Segmentation to Support Automation and System Security

Merista Aulia^{1*}, Nayla Jasmine², Icha Marisa Mahmuda³, Raden Najla Ramadhani⁴, Johannes Hamonangan Siregar⁵

^{1,2,3,4,5}Universitas Pembangunan Jaya (Prodi Sistem Informasi, Fakultas Teknologi dan Desain, Universitas Pembangunan Jaya, Kota Tangerang Selatan, Indonesia)

*E-mail: raden.najlaramadhani@student.upj.ac.id

raden.najlaramadhani@student.upj.ac.id; merista.aulia@student.upj.ac.id;

nayla.jasmine@student.upj.ac.id; icha.marisamahmuda@student.upj.ac.id; johannes.siregar@upj.ac.id

Article History

Submitted : Des 22, 2025

Revised : Juni 9, 2026

Accepted : Juli 11, 2026

Available Online : Juli 31, 2026

Published Regularly : Juli 31, 2026

Kata Kunci: Cisco Packet Tracer; Internet of Things; NDLC; Segmentasi VLAN; Smart Home;

Keywords: Cisco Packet Tracer; Internet of Things; NDLC; Smart Home; VLAN Segmentation;

Contact



Author

raden.najlaramadhani@student.upj.ac.id

ABSTRAK

Internet of Things (IoT) memberi inovasi dalam penerapan sistem smart home untuk meningkatkan kenyamanan, efisiensi energi dan keamanan tempat tinggal. Namun, sistem smart home masih menghadapi permasalahan besar berupa pemborosan energi listrik dan keamanan jaringan akibat banyaknya perangkat IoT berada dalam satu jaringan sehingga memerlukan segmentasi memadai. Penelitian ini bertujuan merancang jaringan IoT smart home untuk meningkatkan efisiensi energi dan keamanan jaringan pada sistem smart home dengan mengaplikasikan segmentasi VLAN menggunakan Cisco Packet Tracer. Pengembangan sistem menggunakan metode model Network Development Life Cycle (NDLC) dengan melaksanakan fase analisis, desain, simulasi, implementasi, monitoring dan management. Simulasi dilakukan dengan menggunakan Cisco Packet Tracer dengan mengintegrasikan perangkat IoT sebanyak 13 buah perangkat berupa smart lamp, smart door, smart garage dan webcam dengan menghubungkan IoT Server sebagai sistem monitoring terpusat. Hasil pengujian menunjukkan bahwa segmentasi VLAN berhasil memisahkan traffic perangkat IoT dan user dengan latency rendah berkisar antara 18-20ms dengan rate konektivitas 100% serta sistem otomasi dan monitoring dapat diakses secara real-time melalui smartphone. Penelitian ini membuktikan bahwa implementasi segmentasi VLAN pada smart home efektif meningkatkan keamanan jaringan IoT

dengan mempertahankan efisiensi komunikasi antar perangkat dengan performa optimal.

ABSTRACT

The Internet of Things (IoT) provides innovation in the application of smart home systems to improve comfort, energy efficiency, and home security. However, smart home systems still face major problems in the form of electricity waste and network security due to the large number of IoT devices in a single network, which requires adequate segmentation. This study aims to design a smart home IoT network to improve energy efficiency and network security in smart home systems by applying VLAN segmentation using Cisco Packet Tracer. The system development uses the Network Development Life Cycle (NDLC) model method by implementing the analysis, design, simulation, implementation, monitoring, and management phases. Simulation was performed using Cisco Packet Tracer by integrating 13 IoT devices, including smart lamps, smart doors, smart garages, and webcams, connected to an IoT server as a centralized monitoring system. The test results showed that VLAN segmentation successfully separated IoT device and user traffic with low latency ranging from 18-20ms with a 100% connectivity rate, and the automation and monitoring systems could be accessed in real-time via a smartphone. This study proves that the implementation of VLAN segmentation in smart homes effectively improves IoT network security while maintaining efficient communication between devices with optimal performance.

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi pada era digital mendorong pemanfaatan **Internet of Things (IoT)** dalam berbagai bidang kehidupan, termasuk pada lingkungan rumah tinggal [1]. Melalui konsep IoT, berbagai perangkat elektronik dapat saling terhubung dan berkomunikasi melalui jaringan internet sehingga mampu bertukar data serta menjalankan fungsi otomatis sesuai kebutuhan pengguna [2]. Salah satu implementasi IoT yang berkembang pesat adalah **smart home**, yaitu sistem yang mengintegrasikan berbagai perangkat rumah tangga untuk meningkatkan kenyamanan, efisiensi penggunaan energi, dan keamanan lingkungan tempat tinggal [3].

Kebutuhan terhadap hunian yang nyaman dan efisien semakin meningkat seiring dengan tingginya mobilitas masyarakat modern. Pengguna menginginkan berbagai perangkat rumah tangga dapat dikendalikan secara otomatis maupun jarak jauh sehingga aktivitas sehari-hari menjadi lebih praktis [4]. Di sisi lain, meningkatnya jumlah perangkat elektronik yang digunakan di dalam rumah menyebabkan konsumsi energi listrik juga semakin besar. Pengoperasian perangkat yang tidak terkontrol berpotensi meningkatkan pemborosan energi dan biaya operasional rumah tangga [5]. Oleh karena itu, diperlukan sistem smart home yang mampu mengotomatisasi pengoperasian perangkat sekaligus mendukung pengelolaan energi secara lebih efisien.

Selain efisiensi energi, aspek keamanan menjadi tantangan penting dalam implementasi smart home. Menurut penelitian sebelumnya, tingkat kejahatan pada lingkungan tempat tinggal mencapai 87,19% dari seluruh tindak kejahatan, sedangkan perangkat IoT pada smart home memiliki kerentanan terhadap berbagai ancaman siber akibat banyaknya perangkat yang beroperasi pada jaringan yang sama tanpa mekanisme segmentasi yang memadai [6]. Kondisi

tersebut menyebabkan gangguan pada satu perangkat berpotensi memengaruhi perangkat lain sehingga meningkatkan risiko akses tidak sah maupun penyebaran serangan di dalam jaringan. Oleh karena itu, diperlukan rancangan jaringan yang tidak hanya mampu mengintegrasikan perangkat IoT, tetapi juga menerapkan segmentasi jaringan untuk meningkatkan keamanan sistem.

Berbagai penelitian terdahulu telah mengembangkan sistem smart home dengan pendekatan yang beragam. Prasetyo dan Dendi [4] melakukan simulasi desain rumah pintar menggunakan Cisco Packet Tracer dengan metode Network Development Life Cycle (NDLC) yang berfokus pada pengendalian perangkat melalui jaringan internal maupun eksternal. Penelitian tersebut menunjukkan bahwa Cisco Packet Tracer dapat digunakan sebagai media simulasi yang efektif dalam merancang konsep smart home tanpa memerlukan perangkat keras secara langsung. Selanjutnya, Putra dan Darwis [7] mengembangkan sistem smart home berbasis Internet of Things (IoT) menggunakan metode Waterfall pada Cisco Packet Tracer dengan memanfaatkan sensor untuk mengendalikan pencahayaan berdasarkan keberadaan penghuni. Penelitian lain oleh Pambudiyatno, Rifai, dan Harianto [8] merancang arsitektur jaringan IoT pada lingkungan pendidikan dengan menitikberatkan pada pengelolaan struktur jaringan sebagai pendukung ekosistem Internet of Things. Meskipun demikian, penelitian-penelitian tersebut masih berfokus pada otomasi perangkat dan rancangan jaringan dasar, sehingga belum mengimplementasikan segmentasi jaringan berbasis **Virtual Local Area Network (VLAN)** sebagai mekanisme untuk mengisolasi perangkat IoT sekaligus mendukung pengendalian perangkat secara aman melalui akses jarak jauh. Kesenjangan tersebut menunjukkan bahwa penerapan VLAN pada jaringan smart home masih memerlukan kajian lebih lanjut.

Penelitian ini memanfaatkan Cisco Packet Tracer sebagai platform simulasi karena mampu menyediakan berbagai perangkat jaringan dan perangkat Internet of Things (IoT) yang dapat dikonfigurasi dalam satu topologi jaringan secara terintegrasi. Kemampuan tersebut memungkinkan proses perancangan, implementasi, dan pengujian sistem dilakukan secara efisien tanpa memerlukan perangkat keras secara langsung [9][10]. Selain mengurangi biaya pengembangan, pendekatan simulasi juga meminimalkan risiko kerusakan perangkat selama proses perancangan serta memudahkan identifikasi permasalahan jaringan sebelum sistem diterapkan pada lingkungan nyata [11]. Simulasi merupakan proses peniruan terhadap kondisi sistem nyata beserta karakteristik perilakunya sehingga dapat digunakan sebagai media pengujian maupun evaluasi rancangan sistem sebelum implementasi sebenarnya [12].

Berdasarkan permasalahan dan kesenjangan penelitian tersebut, penelitian ini bertujuan merancang jaringan IoT smart home dengan menerapkan segmentasi VLAN untuk mendukung otomasi perangkat dan meningkatkan keamanan sistem. Secara khusus penelitian ini bertujuan untuk: (1) merancang topologi jaringan smart home berbasis VLAN sebagai mekanisme segmentasi perangkat IoT; (2) mengimplementasikan otomasi lima smart lamp yang dapat dikendalikan secara lokal maupun jarak jauh untuk mendukung efisiensi penggunaan energi; serta (3) mengintegrasikan empat smart door, satu smart garage door, dan tiga webcam/CCTV sebagai sistem keamanan yang mampu melakukan pemantauan secara real-time dan mendukung deteksi ancaman secara otomatis.

Kontribusi utama penelitian ini terletak pada penerapan segmentasi VLAN pada arsitektur jaringan smart home untuk meningkatkan keamanan komunikasi antarperangkat IoT. Selain itu, penelitian ini mengintegrasikan otomasi pencahayaan, sistem kontrol akses, dan pemantauan berbasis CCTV dalam satu rancangan jaringan yang dapat diakses secara remote. Hasil penelitian diharapkan dapat menjadi referensi dalam pengembangan jaringan smart home yang lebih aman, efisien, dan mudah diimplementasikan melalui pendekatan simulasi sebelum diterapkan pada lingkungan nyata.

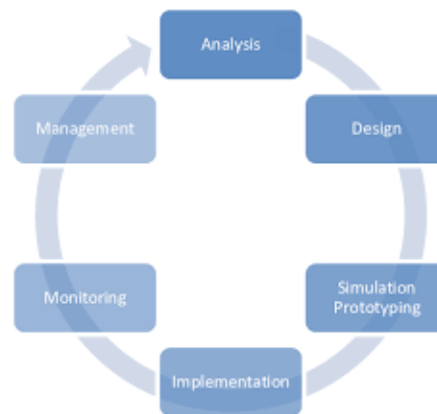
2. Metode Penelitian

Penelitian ini menggunakan metode simulasi untuk merancang dan menguji jaringan Internet of Things (IoT) pada sistem smart home menggunakan Cisco Packet Tracer. Pendekatan simulasi dipilih karena mampu merepresentasikan kondisi jaringan secara mendekati

implementasi nyata tanpa memerlukan perangkat keras, sehingga proses perancangan, konfigurasi, dan pengujian dapat dilakukan secara lebih efisien dengan risiko implementasi yang lebih rendah. Pengembangan jaringan dilakukan menggunakan metode **Network Development Life Cycle (NDLC)** yang terdiri atas enam tahapan, yaitu analysis, design, simulation prototype, implementation, monitoring, dan management. Metode NDLC dipilih karena menyediakan alur pengembangan jaringan yang sistematis, mulai dari identifikasi kebutuhan hingga evaluasi hasil implementasi[13][14].

2.1 Metode Pengembangan

Pengembangan jaringan IoT smart home dilaksanakan mengikuti tahapan NDLC sebagaimana ditunjukkan pada Gambar 1.



Gambar 1. *Network Development Life Cycle (NDLC)*

1. Analysis

Tahap analysis dilakukan untuk mengidentifikasi kebutuhan sistem berdasarkan karakteristik smart home yang akan dibangun. Analisis meliputi identifikasi kebutuhan perangkat IoT, infrastruktur jaringan, kebutuhan pengguna, serta mekanisme segmentasi jaringan untuk meningkatkan keamanan komunikasi antarperangkat. Selain itu dilakukan studi literatur terhadap penelitian terdahulu sebagai dasar dalam menentukan rancangan topologi, konfigurasi jaringan, dan metode pengujian yang digunakan.

2. Design

Tahap design bertujuan menyusun arsitektur jaringan smart home berdasarkan hasil analisis. Pada tahap ini dirancang topologi jaringan yang terdiri atas router, Layer-3 switch, access point, server IoT, smartphone pengguna, serta perangkat IoT. Selain itu ditentukan skema segmentasi jaringan menggunakan Virtual Local Area Network (VLAN), pengalamatan IP, serta mekanisme inter-VLAN routing yang digunakan sebagai dasar implementasi sistem.

3. Simulation Prototype

Pada tahap simulation prototype seluruh rancangan jaringan diimplementasikan menggunakan Cisco Packet Tracer. Seluruh perangkat jaringan dan perangkat IoT dikonfigurasi sesuai desain sehingga dapat dilakukan validasi awal terhadap konektivitas jaringan, komunikasi antarperangkat, serta fungsi otomatisasi sebelum dilakukan pengujian secara menyeluruh.

4. Implementation

Tahap implementation dilakukan dengan mengonfigurasi seluruh perangkat jaringan sesuai rancangan yang telah dibuat. Konfigurasi meliputi pembuatan VLAN, konfigurasi trunk, interface VLAN (SVI), inter-VLAN routing pada Layer-3 switch, konfigurasi access point, server IoT, serta pengalamatan IP pada seluruh perangkat agar sistem dapat beroperasi sesuai kebutuhan.

5. Monitoring

Tahap monitoring dilakukan untuk mengamati kinerja jaringan selama simulasi berlangsung. Pengamatan difokuskan pada konektivitas antarperangkat, keberhasilan komunikasi antar-VLAN, fungsi otomatisasi perangkat IoT, serta kemampuan sistem dalam memberikan layanan sesuai skenario yang telah dirancang.

6. Management

Tahap management dilakukan melalui evaluasi hasil konfigurasi dan pengujian jaringan untuk memastikan rancangan memenuhi aspek keandalan, kemudahan pengelolaan, dan kesiapan implementasi pada lingkungan nyata. Tahap ini juga menghasilkan rekomendasi pengembangan sebagai penyempurnaan rancangan jaringan.

2.2 Tahap Pengembangan

Dalam tahap pengembangan diterapkan metode NDLC secara bertahap untuk memastikan pengembangan jaringan IoT *smart home* dilakukan secara terstruktur dan sistematis. Berikut adalah detail implementasi dari setiap tahapan pengembangan.

2.2.1 Spesifikasi Kebutuhan Sistem

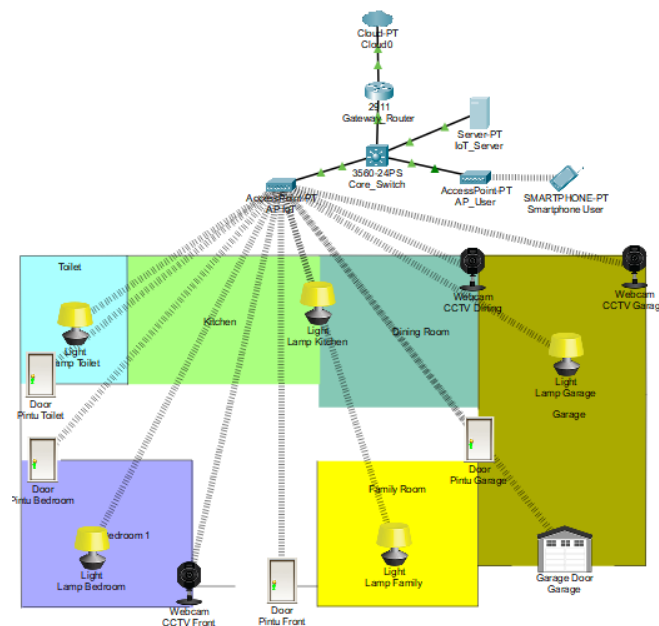
Berdasarkan tahap analisis yang telah dilakukan, berikut adalah hasil indentifikasi sistem yang mencakup perangkat IoT dan infrastruktur jaringan. Spesifikasi lengkap kebutuhan perangkat dapat dilihat pada Tabel 1.

Tabel 1. Spesifikasi Kebutuhan Perangkat IoT dan Infrastruktur Jaringan

Kategori	Perangkat	Jumlah	Fungsi Utama
Pencahaya	Smart Lamp	5	Pencayaan berbasis smartphone
Keamanan	Smart Door	4	Kontrol Buka/Kunci Pintu
Keamanan	Smart Garage Door	1	Kontrol Buka/Kunci Pintu garasi
Keamanan	Webcam/CCTV	3	Monitoring visual real-time
Infrastruktur	Cloud	1	Simulasi koneksi internet eksternal
Infrastruktur	Router	1	Penyediaan jaringan local ke internet
Infrastruktur	Core Switch	1	Manajemen VLAN
Infrastruktur	Access Point	2	Akses nirkabel
Infrastruktur	Server	1	Pusat monitoring dan manajemen perangkat IoT
User Device	Smartphone	1	Interface kontrol pengguna

2.2.2 Desain Topologi Jaringan

Desain topologi jaringan *smart home* bergantung pada implementasi server IoT, yang berfungsi sebagai sistem manajemen pusat yang terhubung ke switch lapisan 3. Switch lapisan 3 menyediakan segmentasi dalam VLAN dan routing antar-VLAN. Router nirkabel terhubung ke switch untuk menyediakan konektivitas nirkabel. Topologi jaringan lengkap dapat dilihat pada Gambar 2.



Gambar 2. Topologi Jaringan *Smart Home*

Segmentasi VLAN dirancang untuk memisahkan traffic jaringan berdasarkan fungsi perangkat. Konfigurasi detail setiap VLAN dapat dilihat pada Tabel 2.

Tabel 2. Konfigurasi Segmentasi VLAN *Smart Home*

VLAN ID	Nama VLAN	Network Address	Subnet Mask	Default Gateway
10	IoT_Device	192.168.10.0/24	255.255.255.0	192.168.10.1
20	User_Device	192.168.20.0/24	255.255.255.0	192.168.20.1

2.2.3 Konfigurasi Perangkat Jaringan

Konfigurasi perangkat jaringan dilakukan untuk memastikan sistem jaringan dapat berjalan sesuai dengan kebutuhan fungsional, baik dari sisi segmentasi jaringan, komunikasi anatarperangkat maupun keamanan akses. Konfigurasi ini mencakup paengaturan VLAN, inter-VLAN routing, access point, serta pengamatan IP pada seluruh perangkat jaringan.

a. Konfigurasi *Virtual Local Area* (VLAN)

Segmentasi jaringan dilaksanakan melalui *Virtual Local Area* (VLAN) dengan tujuan memisahkan jaringan berdasarkan jenis perangkat, pembagian segmentasi ini bertujuan untuk meningkatkan efisiensi pengelolaan jaringan [15][4].

b. Konfigurasi Inter-VLAN Routing

Untuk memungkinkan komunikasi inter device yang terdiri dari VLAN yang berada pada VLAN yang lain, dilakukan konfigurasi inter-VLAN routing dengan menggunakan *core switch*. Pada setiap VLAN dilakukan pembentukan interface VLAN yang menjadi gateway defaultnya.

c. Konfigurasi Access Point

Access point dikonfigurasi agar memberikan akses jaringan nirkabel berdasarkan segmentasi VLAN yang telah dibentuk sebelumnya. Setiap SSID terhubung dengan VLAN yang berbeda satu dengan lainnya agar mencegah isolasi jaringan bagi jenis perangkat yang berbeda.

d. Konfigurasi Alamat IP

Konfigurasi IP menggunakan IP static untuk memastikan bahwa setiap alat memiliki IP address yang sama dan bisa dikelola dengan mudah.

2.2.4 Metode Pengujian

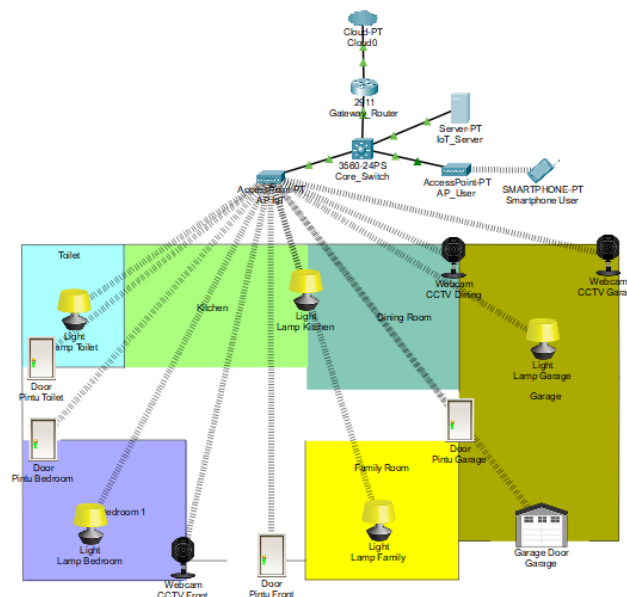
Pengujian sistem ini dilakukan dengan metode simulation-based testing yang mencakup tiga kategori:

- a. Pengujian Konektivitas Antar VLAN
Pengujian konektivitas dilakukan dengan ping-test untuk memverifikasi komunikasi antar perangkat dan memastikan bahwa inter-VLAN routing pada core switch telah berjalan dengan baik. Pengujian ini dilakukan dengan cara ping dari perangkat pada VLAN 10 (IoT_Device) ke perangkat pada VLAN 20 (User_Devices) dan sebaliknya.
- b. Pengujian Fungsionalitas Perangkat IoT
Pengujian fungsionalitas dilakukan untuk setiap jenis perangkat dan memastikan smartphone dapat mengakses seluruh perangkat IoT yang terhubung ke jaringan. Pengujian ini dilakukan dengan cara mengirim perintah ping dari smartphone ke masing-masing perangkat IoT yang berada pada VLAN 10.
- c. Verifikasi Inter-VLAN Routing
Verifikasi Inter-VLAN routing dilakukan untuk memastikan bahwa proses routing antar-VLAN berjalan dengan baik pada core switch. Verifikasi ini dilakukan untuk mengamati jalur komunikasi data saat proses ping berlangsung dan memastikan bahwa setiap perangkat menggunakan default gateway yang sesuai

3. Hasil dan Pembahasan

3.1 Hasil Implementasi Topologi Jaringan *Smart Home*

Implementasi topologi jaringan *smart home* berbasis VLAN telah berhasil dilakukan menggunakan Cisco Packet Tracer. Topologi yang dibangun terdiri dari 1 Cloud, 1 Gateway Router, 1 Multilayer Switch 3560-24PS sebagai core switch, 2 Access Point, 1 IoT Server, 13 perangkat IoT, dan 1 smartphone sebagai user device. Gambar 3 menunjukkan topologi lengkap yang telah diimplementasikan.



Gambar 3. Topologi Jaringan *Smart Home*

Arsitektur jaringan menggunakan konsep segmentasi VLAN untuk memisahkan traffic antara perangkat IoT dan perangkat user. VLAN 10 (192.168.10.0/24) dialokasikan untuk IoT Server dan 13 IoT devices yang terdiri dari 5 smart lamp, 4 smart door , 3 webcam, dan 1 smart garage door. Sedangkan VLAN 20 (192.168.20.0/24) dialokasikan untuk user devices yaitu smartphone. IoT Server berfungsi sebagai central monitoring system yang menghubungkan smartphone dengan semua perangkat IoT.

3.2 Konfigurasi VLAN pada Multilayer Switch

Port FastEthernet 0/1 dan Fa0/2 di-assign ke VLAN 10 untuk koneksi ke AP_IoT, port Fa0/5 di-assign ke VLAN 10 untuk IoT Server, sedangkan port FastEthernet 0/24 di-assign ke VLAN 20 untuk koneksi ke AP_User. Gambar 4 menunjukkan Hasil Show VLAN Brief di Core Switch.

```

Core_Switch
Core_Switch>enable
Core_Switch#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/3, Fa0/4, 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
                                           Gig0/2
10   IoT_Devices             active    Fa0/1, Fa0/2, Fa0/5
20   User_Devices            active    Fa0/24
1002 fddi-default            active
1003 token-ring-default    active
1004 fddinet-default        active
1005 trnet-default          active
Core_Switch#
  
```

Gambar 4. Hasil Show VLAN Brief di Core Switch

Hasil verifikasi konfigurasi VLAN menunjukkan bahwa VLAN 10 memiliki port Fa0/1, Fa0/2, dan Fa0/5, sedangkan VLAN 20 memiliki port Fa0/24. Kedua VLAN dalam status active dan port-port telah ter-assign dengan benar sesuai rancangan. Tabel 1. menunjukkan ringkasan konfigurasi VLAN yang telah diterapkan.

Tabel 3. Konfigurasi VLAN

VLAN ID	Nama VLAN	Network	Gateway	Port Assignment
10	IoT_Devices	192.168.10.0/24	192.168.10.1	Fa0/1, Fa0/2, Fa0/5
20	User_Devices	192.168.20.0/24	192.168.20.1	Fa0/24

3.3 Konfigurasi Inter-VLAN Routing

Inter-VLAN routing dikonfigurasi menggunakan Switched Virtual Interface (SVI) pada Multilayer Switch. Interface VLAN 10 diberikan IP address 192.168.10.1 sebagai default gateway untuk perangkat IoT, sedangkan interface VLAN 20 diberikan IP address 192.168.20.1 sebagai default gateway untuk user devices. Fitur IP routing diaktifkan pada Core Switch untuk memungkinkan komunikasi antar VLAN. Gambar 5. Menunjukan hasil Show ip interface brief di Core Switch

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	up	up
FastEthernet0/6	unassigned	YES	unset	down	down
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down
FastEthernet0/13	unassigned	YES	unset	down	down
FastEthernet0/14	unassigned	YES	unset	down	down
FastEthernet0/15	unassigned	YES	unset	down	down
FastEthernet0/16	unassigned	YES	unset	down	down
FastEthernet0/17	unassigned	YES	unset	down	down
FastEthernet0/18	unassigned	YES	unset	down	down
FastEthernet0/19	unassigned	YES	unset	down	down
FastEthernet0/20	unassigned	YES	unset	down	down
FastEthernet0/21	unassigned	YES	unset	down	down
FastEthernet0/22	unassigned	YES	unset	down	down
FastEthernet0/23	unassigned	YES	unset	down	down
FastEthernet0/24	unassigned	YES	unset	up	up
GigabitEthernet0/1	192.168.1.2	YES	manual	up	up
GigabitEthernet0/2	unassigned	YES	unset	down	down
Vlan1	unassigned	YES	unset	up	up
Vlan10	192.168.10.1	YES	manual	up	up
Vlan20	192.168.20.1	YES	manual	up	up

Gambar 5. Hasil Show ip interface brief di Core Switch

Dengan konfigurasi ini, perangkat pada VLAN 10 dan VLAN 20 dapat saling berkomunikasi melalui proses routing di Multilayer Switch tanpa memerlukan router eksternal.

3.4 Konfigurasi Access Point dan Konektivitas Wireless

Dua Access Point dikonfigurasi untuk menyediakan konektivitas wireless. AP_IoT dikonfigurasi dengan SSID "HomeGateway" menggunakan enkripsi WPA2-PSK dengan password "smarthomesales". Access Point ini terhubung ke Core Switch melalui port Fa0/1 yang berada di VLAN 10. Gambar 6. menampilkan konfigurasi AP_IoT.

AP IoT

Physical Config Attributes

GLOBAL

Settings

INTERFACE

Port 0

Port 1

Port 1

Port Status ☒ On

SSID HomeGateway

2.4 GHz Channel 6

Coverage Range (meters) 140,00

Authentication

☐ Disabled ☐ WEP ☒ WPA2-PSK

WEP Key

PSK Pass Phrase smarthomesales

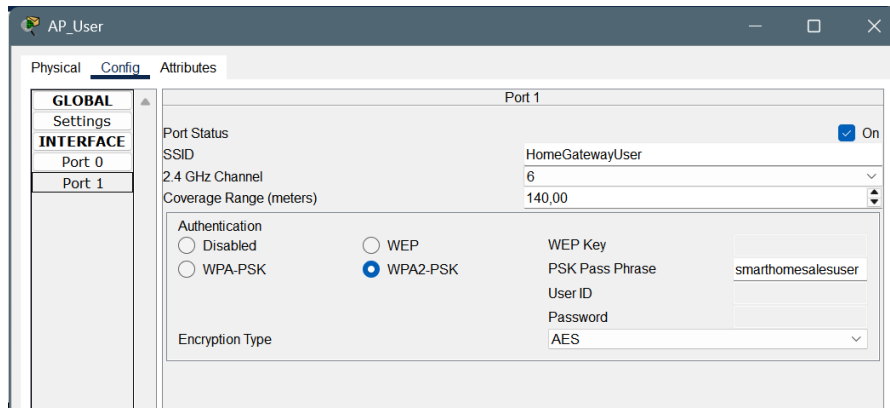
User ID

Password

Encryption Type AES

Gambar 6. Konfigurasi AP_IoT

AP_User dikonfigurasi dengan SSID "HomeGatewayUser" juga menggunakan enkripsi WPA2-PSK. Access Point ini terhubung ke port Fa0/24 yang berada di VLAN 20. Penggunaan dua Access Point terpisah memastikan segmentasi wireless traffic sesuai dengan segmentasi VLAN yang telah dirancang, sehingga meningkatkan keamanan dan mengurangi interferensi antar traffic. Gambar 7. menampilkan konfigurasi AP_User



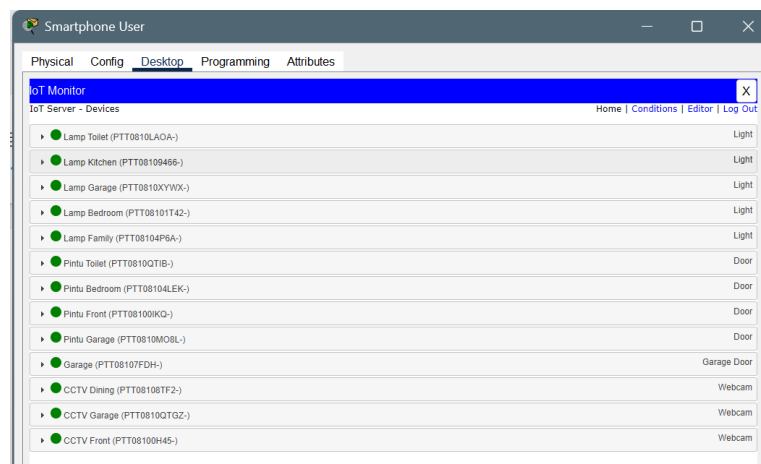
Gambar 7. Konfigurasi AP_User

3.5 Konfigurasi IoT Devices dan Registrasi ke Server

Sebanyak 13 perangkat IoT dikonfigurasi dengan IP static (192.168.10.21-192.168.10.51). Setiap device diregistrasi ke IoT Server dengan konfigurasi remote server: Server Address 192.168.10.10, Username "sales", Password "salesroti". Tabel 4. Menunjukkan Daftar Perangkat IoT dan Gambar 8. menampilkan Konfigurasi remote server di IoT device.

Tabel 4. Daftar Perangkat IoT

Perangkat	Lokasi	IP Address	Status
Door	Toilet	192.168.10.21	Connected
Door	Kitchen	192.168.10.22	Connected
Door	Bedroom	192.168.10.23	Connected
Door	Front	192.168.10.24	Connected
Garage Door	Garage	192.168.10.25	Connected
Lamp	Toilet	192.168.10.31	Connected
Lamp	Kitchen	192.168.10.32	Connected
Lamp	Bedroom	192.168.10.33	Connected
Lamp	Family	192.168.10.34	Connected
Lamp	Garage	192.168.10.35	Connected
Webcam	Dining	192.168.10.41	Connected
Webcam	Garage	192.168.10.42	Connected
Webcam	Front	192.168.10.43	Connected



Gambar 8. Konfigurasi remote server di IoT device

3.7 Pengujian Konektivitas

3.7.1 Pengujian Inter-VLAN Routing

Ping dari smartphone (192.168.20.100) ke gateway VLAN 10 (192.168.10.1) menunjukkan success rate 100% (4/4) dengan rata-rata RTT 20ms. Gambar 9. Hasil ping smartphone ke gateway VLAN 10

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=16ms TTL=255
Reply from 192.168.10.1: bytes=32 time=12ms TTL=255
Reply from 192.168.10.1: bytes=32 time=11ms TTL=255
Reply from 192.168.10.1: bytes=32 time=61ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 61ms, Average = 25ms

C:\>
```

Gambar 9. Hasil ping smartphone ke gateway VLAN 10

3.7.2 Pengujian Konektivitas ke IoT Server

Ping dari smartphone ke IoT Server (192.168.10.10) menunjukkan success rate 100% (4/4) dengan rata-rata RTT 18ms. Login aplikasi IoT Monitor berhasil dan real-time monitoring berfungsi dengan baik. Gambar 10. menunjukkan hasil ping smartphone ke IoT Server

```
C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.10.10: bytes=32 time=41ms TTL=127
Reply from 192.168.10.10: bytes=32 time=18ms TTL=127
Reply from 192.168.10.10: bytes=32 time=37ms TTL=127
Reply from 192.168.10.10: bytes=32 time=28ms TTL=127

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 41ms, Average = 31ms
```

Gambar 10. Hasil ping smartphone ke IoT Server

3.7.3 Pengujian Konektivitas ke IoT Devices

Ping dari smartphone ke IoT devices menunjukkan success rate 100% setelah konfigurasi gateway diperbaiki. Pengujian dari Core Switch ke semua perangkat IoT juga menunjukkan success rate 100% (5/5). Gambar 11. Menunjukkan hasil ping ke IoT devices

```

C:\>ping 192.168.10.21

Pinging 192.168.10.21 with 32 bytes of data:

Reply from 192.168.10.21: bytes=32 time=45ms TTL=254
Reply from 192.168.10.21: bytes=32 time=55ms TTL=254
Reply from 192.168.10.21: bytes=32 time=54ms TTL=254
Reply from 192.168.10.21: bytes=32 time=58ms TTL=254

Ping statistics for 192.168.10.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 45ms, Maximum = 58ms, Average = 53ms

C:\>ping 192.168.10.31

Pinging 192.168.10.31 with 32 bytes of data:

Reply from 192.168.10.31: bytes=32 time=39ms TTL=254
Reply from 192.168.10.31: bytes=32 time=25ms TTL=254
Reply from 192.168.10.31: bytes=32 time=11ms TTL=254
Reply from 192.168.10.31: bytes=32 time=33ms TTL=254

Ping statistics for 192.168.10.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 39ms, Average = 27ms

C:\>ping 192.168.10.41

Pinging 192.168.10.41 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.41: bytes=32 time=41ms TTL=254
Reply from 192.168.10.41: bytes=32 time=43ms TTL=254
Reply from 192.168.10.41: bytes=32 time=40ms TTL=254

Ping statistics for 192.168.10.41:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 40ms, Maximum = 43ms, Average = 41ms

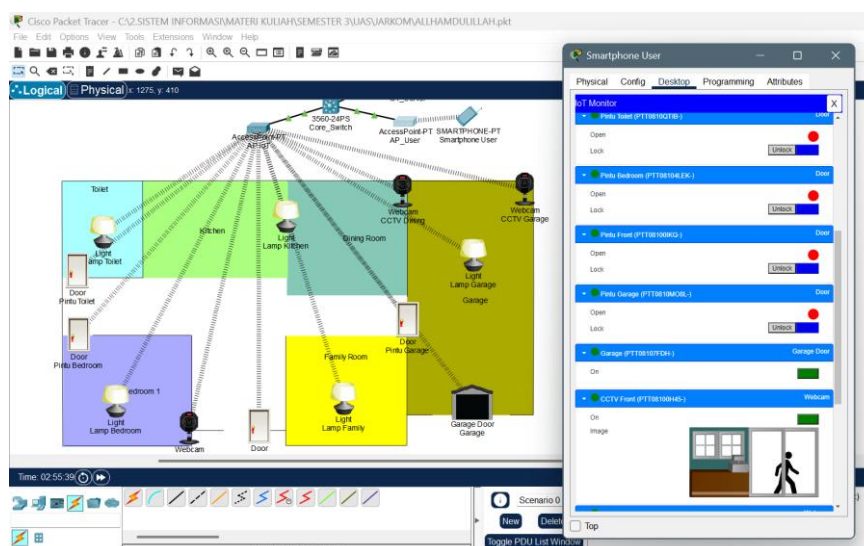
C:\>|

```

Gambar 11. Hasil ping ke IoT devices

3.7.4 Pengujian Kontrol Perangkat

Kontrol perangkat melalui aplikasi IoT Monitor menunjukkan response time < 2 detik untuk semua operasi (ON/OFF lampu, buka/tutup pintu, monitoring CCTV) dengan success rate 100%.



Gambar 12. Pengujian kontrol perangkat via IoT Monitor

3.8 Analisis Hasil

Hasil implementasi menunjukkan beberapa temuan penting:

- a. Efektivitas Segmentasi VLAN: Traffic IoT dan user terpisah secara logical namun tetap dapat berkomunikasi melalui inter-VLAN routing, meningkatkan keamanan sistem.
- b. Performa Inter-VLAN Routing: Latency rendah (18-20ms) menunjukkan efisiensi hardware-based routing pada Multilayer Switch.
- c. Central Monitoring System: IoT Server memberikan arsitektur terstruktur dengan manajemen terpusat, memudahkan logging dan troubleshooting.
- d. Keamanan Autentikasi: Mekanisme autentikasi dengan username/password mencegah akses tidak sah ke sistem.
- e. Konektivitas Wireless: Semua 13 perangkat IoT terhubung wireless dengan signal strength baik, memberikan fleksibilitas penempatan perangkat.

3.9 Pembahasan

Hasil implementasi menunjukkan bahwa penerapan segmentasi **Virtual Local Area Network (VLAN)** mampu meningkatkan keamanan jaringan smart home tanpa mengurangi kualitas komunikasi antarperangkat. Pemisahan perangkat IoT ke dalam VLAN 10 dan perangkat pengguna ke dalam VLAN 20 membentuk dua **broadcast domain** yang berbeda. Kondisi ini menyebabkan lalu lintas broadcast hanya beredar pada masing-masing segmen jaringan sehingga perangkat yang berada pada VLAN lain tidak dapat menerima broadcast tersebut secara langsung. Selain meningkatkan efisiensi penggunaan bandwidth, mekanisme ini juga mengurangi peluang penyebaran serangan jaringan, seperti *broadcast flooding* maupun perpindahan akses tidak sah dari satu kelompok perangkat ke kelompok lainnya. Komunikasi antarsegmen tetap dapat berlangsung melalui mekanisme **inter-VLAN routing** pada Layer-3 switch sehingga akses pengguna terhadap perangkat IoT tetap terjaga.

Nilai *round-trip time* (RTT) sebesar 18–20 ms pada pengujian konektivitas menunjukkan bahwa proses komunikasi antar-VLAN berlangsung dengan latensi yang rendah. Kondisi ini dipengaruhi oleh penggunaan Layer-3 switch sebagai perangkat routing yang melakukan proses forwarding secara langsung pada perangkat keras (*hardware-based switching*), sehingga waktu pemrosesan paket menjadi lebih singkat dibandingkan apabila menggunakan router konvensional. Selain itu, pemisahan perangkat ke dalam dua VLAN juga mengurangi jumlah lalu lintas broadcast pada masing-masing segmen sehingga beban komunikasi jaringan menjadi lebih ringan dan proses pertukaran data berlangsung lebih efisien.

Keberhasilan seluruh pengujian konektivitas dengan *success rate* sebesar 100% menunjukkan bahwa konfigurasi VLAN, inter-VLAN routing, pengalamatan IP statis, serta konfigurasi *default gateway* telah diterapkan secara konsisten. Kondisi tersebut memungkinkan smartphone pada VLAN pengguna tetap dapat mengakses server IoT dan seluruh perangkat IoT melalui mekanisme routing yang telah dikonfigurasi. Hasil ini menunjukkan bahwa penerapan segmentasi jaringan tidak menghambat fungsi otomatis, tetapi justru memberikan pemisahan akses yang lebih terkontrol tanpa mengurangi kemudahan pengelolaan perangkat.

Selain itu, penggunaan server IoT sebagai pusat pengelolaan perangkat memberikan keuntungan berupa arsitektur komunikasi yang lebih terstruktur. Seluruh proses autentikasi, monitoring, dan pengendalian perangkat dilakukan melalui satu titik layanan sehingga memudahkan proses administrasi, pemantauan, serta pengembangan sistem pada masa mendatang. Pendekatan ini lebih mudah dipelihara dibandingkan komunikasi langsung (*peer-to-peer*) antarperangkat, terutama ketika jumlah perangkat IoT terus bertambah.

Hasil penelitian ini melengkapi penelitian Prasetyo dan Dendi [4] yang berhasil membangun simulasi smart home menggunakan Cisco Packet Tracer, namun masih berfokus pada otomatisasi perangkat tanpa menerapkan segmentasi jaringan berbasis VLAN. Penelitian Putra dan Darwis [7] juga berhasil mengembangkan sistem smart home berbasis IoT dengan memanfaatkan sensor otomatis, tetapi belum membahas mekanisme isolasi jaringan sebagai bagian dari aspek keamanan. Sementara itu, penelitian Pambudiyatno, Rifai, dan Harianto[8] telah menekankan pentingnya perancangan arsitektur jaringan IoT, tetapi implementasinya lebih diarahkan pada lingkungan pendidikan dan belum mengintegrasikan otomatisasi smart home dengan segmentasi jaringan.

Dibandingkan penelitian-penelitian tersebut, penelitian ini memberikan kontribusi melalui integrasi tiga aspek utama, yaitu penerapan segmentasi VLAN untuk meningkatkan keamanan komunikasi jaringan, implementasi inter-VLAN routing yang tetap memungkinkan akses antarperangkat secara terkendali, serta integrasi server IoT sebagai pusat monitoring dan pengendalian seluruh perangkat smart home. Kombinasi tersebut menghasilkan arsitektur jaringan yang tidak hanya mendukung otomasi perangkat secara real-time, tetapi juga memberikan keamanan jaringan yang lebih baik serta kemudahan dalam pengelolaan sistem. Secara keseluruhan, hasil penelitian menunjukkan bahwa penerapan segmentasi VLAN pada jaringan smart home merupakan pendekatan yang efektif untuk meningkatkan keamanan komunikasi antarperangkat tanpa menurunkan performa jaringan. Arsitektur yang dihasilkan juga memiliki potensi untuk dikembangkan pada implementasi smart building maupun lingkungan Internet of Things yang memiliki jumlah perangkat lebih banyak dengan tetap mempertahankan kemudahan pengelolaan dan skalabilitas sistem.

4. Kesimpulan

Penelitian ini berhasil merancang dan mengimplementasikan jaringan IoT smart home berbasis segmentasi Virtual Local Area Network (VLAN) menggunakan Cisco Packet Tracer dengan metode Network Development Life Cycle (NDLC). Hasil pengujian menunjukkan bahwa segmentasi VLAN mampu mengisolasi komunikasi antara perangkat IoT dan perangkat pengguna sehingga meningkatkan keamanan jaringan tanpa mengurangi kualitas komunikasi antarperangkat. Konfigurasi inter-VLAN routing memungkinkan akses yang terkontrol dengan tingkat keberhasilan konektivitas sebesar 100% dan rata-rata *round-trip time* (RTT) sebesar 18–20 ms. Selain itu, sistem berhasil mengintegrasikan 13 perangkat IoT yang terdiri atas smart lamp, smart door, smart garage door, dan webcam melalui IoT Server sebagai pusat monitoring dan pengendalian. Seluruh perangkat dapat diakses menggunakan smartphone dengan waktu respons kurang dari 2 detik, sehingga menunjukkan bahwa arsitektur yang dirancang mampu mendukung otomasi dan monitoring secara real-time.

Penelitian ini memberikan kontribusi pada penerapan segmentasi VLAN sebagai mekanisme peningkatan keamanan jaringan smart home yang tetap mempertahankan efisiensi komunikasi serta kemudahan pengelolaan perangkat melalui arsitektur client-server. Pemanfaatan Cisco Packet Tracer juga terbukti efektif sebagai media simulasi untuk memvalidasi rancangan jaringan sebelum diterapkan pada perangkat fisik, sehingga dapat menekan biaya dan risiko implementasi. Untuk pengembangan selanjutnya, penelitian dapat diarahkan pada penerapan Access Control List (ACL) untuk memperkuat kebijakan keamanan, implementasi Quality of Service (QoS) guna memprioritaskan trafik penting seperti CCTV, serta pengujian pada perangkat keras nyata agar diperoleh gambaran performa sistem pada kondisi operasional sesungguhnya. Selain itu, integrasi teknologi kecerdasan buatan berpotensi meningkatkan kemampuan otomasi dan adaptasi sistem terhadap pola aktivitas pengguna.

Daftar Pustaka

- [1] C. Anggeliani, J. Angreyani, And Y. Pernando, “Simulasi Topologi Jaringan Berbasis Iot Untuk Perangkat Rumah Tangga Menggunakan Cisco Packet Tracer,” 2025. [Online]. Available: [Http://Jurnal.Goretanpena.Com/Index.Php/Jssr](http://Jurnal.Goretanpena.Com/Index.Php/Jssr)
- [2] S. Megawati And A. Lawi, “Pengembangan Sistem Teknologi Internet Of Things Yang Perlu Dikembangkan Negara Indonesia.”
- [3] M. Suryanto, F. Ardianto, And B. Alfaresi, “Rancang Bangun Sistem Smarthome Berbasis Internet Of Things Dengan Node Mcu Dan Google Assistant Di Smartphone Android.”
- [4] S. E. Prasetyo And D. Dendi, “Simulasi Rancangan Smart Home System Menggunakan Cisco Packet Tracer,” *Jurnal Digital Teknologi Informasi*, Vol. 6, No. 2, Sep. 2023, Doi: 10.32502/Digital.V6i2.5396.
- [5] A. Malik Alrasyid, N. Rahma Diasri, D. Ulandari, And R. Putra Laksana, “Pengaruh Teknologi Internet Of Things (Iot) Terhadap Efisiensi Energi Di Smart Home,” 2025.

- [6] J. Wardoyo, N. Hudallah, And A. B. Utomo, "Smart Home Security System Berbasis Mikrokontroler," *Jurnal Simetris*, Vol. 10, No. 1, 2019.
- [7] A. P. Putra And M. Darwis, "Perancangan Jaringan Sistem Smart Home Berbasis Iot Menggunakan Cisco Packet Tracer Dengan Metode Waterfall," *Jurnal Teknologi Dan Sistem Informasi Bisnis*, Vol. 7, No. 3, Pp. 410–418, Jul. 2025, Doi: 10.47233/Jteksis.V7i3.2015.
- [8] N. Pambudiyatno, M. Rifai, B. B. H. Politeknik, And P. Surabaya, "Desain Jaringan Internet Of Things (Iot) Di Politeknik Penerbangan Surabaya," Bulan Juni, 2021.
- [9] Y. Kurniawan, M. R. Maliki, I. Pebrianto, E. Saputra, A. Z. Ardhana, And M. H. Purwidianoro, "Seminar Nasional Amikom Surakarta (Semnasa) 2024."
- [10] Y. Kurniawan, M. R. Maliki, I. Pebrianto, E. Saputra, A. Z. Ardhana, And M. H. Purwidianoro, "Seminar Nasional Amikom Surakarta (Semnasa) 2024."
- [11] P. Wang And H. Zare, "Teaching Internet Of Things (Iot) Through Software Simulations With Packet Tracer," *Issues In Information Systems*, Vol. 21, No. 2, Pp. 123–134, 2020, Doi: 10.48009/2_Iis_2020_123-134.
- [12] A. W. Putra Eko, M. P. Niko Sona, A. Fauzi Saputra, And D. Rolliawati Universitas Islam Negeri Sunan Ampel Surabaya, "Menggunakan Model Multi Channel-Multi Phase."
- [13] T. Sanjaya And D. Setiyadi, "1-10 Teknik Informatika; Stmik Bina Insani."
- [14] F. Hari Prasetyo, E. Infitharina, And M. Febriyansyah, "Penerapan Metode Network Development Life Cycle (Ndlc) Dalam Pengembangan Jaringan Komputer," *Juni 2025 Journal Of Informatics And Communications Technology*, Vol. 7, No. 1, Pp. 80–087, Doi: 10.52661.
- [15] U. Bumigora Menggunakan Vlan Untuk Ruang Kelas Cerdas Farhan, "Seminar Nasional Corisindo Desain Arsitektur Jaringan Iot Terintegrasi Pada Smart Campus."