

Implementasi Smart Home Berbasis IoT: Studi Simulasi Menggunakan Cisco Packet Tracer

IoT-Based Smart Home Implementation: A Simulation Study Using Cisco Packet Tracer

Ondihon Parlinggoman Munthe¹, Alz Danny Wowor²

^{1,2,3,4}Program Studi Teknik Informatika, FTI, Universitas Kristen Satya Wacana, Salatiga
E-mail: 1672020270@student.uksw.edu, 2alzdanny.wowor@uksw.edu

Abstrak

Pesatnya perkembangan teknologi Internet of Things (IoT) memungkinkan pengendalian perangkat rumah secara otomatis dan jarak jauh. Namun, implementasi langsung pada perangkat keras seringkali membutuhkan biaya tinggi dan konfigurasi yang kompleks. Penelitian ini bertujuan merancang dan menganalisis kinerja sistem Smart Home melalui pendekatan simulasi menggunakan perangkat lunak Cisco Packet Tracer. Metode yang digunakan meliputi perancangan topologi jaringan, konfigurasi layanan jaringan inti, serta pengujian fungsionalitas dan kualitas jaringan (*Quality of Service/QoS*) untuk memvalidasi rancangan tersebut. Hasil simulasi menunjukkan bahwa sistem yang dibangun mampu berjalan dengan baik, di mana *Smartphone* berhasil mengontrol perangkat elektronik secara *real-time*. Pengujian QoS mencatat *packet loss* sebesar 0% dan rata-rata latensi sebesar 27 ms, yang mengindikasikan konektivitas andal antara perangkat pengguna dan server IoT. Studi ini menyimpulkan bahwa simulasi menggunakan Cisco Packet Tracer efektif sebagai tahap validasi awal dalam perancangan infrastruktur Smart Home sebelum implementasi fisik dilakukan.

Kata kunci: *Smart Home, Internet of Things (IoT), Cisco Packet Tracer, Simulasi Jaringan, Latensi.*

Abstract

The rapid development of Internet of Things (IoT) technology enables automatic and remote control of home appliances. However, direct hardware implementation often entails high costs and complex configurations. This study aims to design and analyze the performance of a Smart Home system through a simulation approach using Cisco Packet Tracer software. The method encompasses network topology design, core network service configuration, and functionality and Quality of Service (QoS) testing to validate the proposed design. Simulation results demonstrate that the constructed system operates successfully, with the Smartphone effectively controlling electronic devices in real-time. QoS testing recorded 0% packet loss and an average latency of 27 ms, indicating reliable connectivity between user devices and the IoT Server. This study concludes that simulation using Cisco Packet Tracer is effective as a preliminary validation stage in designing Smart Home infrastructure before physical implementation.

Keywords: *Smart Home, Internet of Things (IoT), Cisco Packet Tracer, Network Simulation, Latency*

1. PENDAHULUAN

Perkembangan teknologi Internet of Things (IoT) telah merevolusi interaksi manusia dengan lingkungan hunian melalui konsep smart home, di mana perangkat seperti lampu, AC, dan sensor keamanan saling terintegrasi untuk meningkatkan

efisiensi energi, keamanan, serta kenyamanan. Secara global, pasar smart home diproyeksikan mencapai US\$175,1 miliar pada 2026 dengan tingkat pertumbuhan tahunan majemuk (CAGR) sebesar 8,82%, didorong oleh lonjakan jumlah perangkat IoT yang terhubung mencapai 21,1 miliar unit pada 2025. Tren ini mencerminkan relevansi ilmiah dalam pengembangan arsitektur jaringan IoT serta manfaat praktis seperti penghematan energi hingga 30% di rumah tangga pintar.

Di Indonesia, adopsi smart home mengalami pertumbuhan pesat dengan nilai pasar mencapai US\$1,81 miliar pada 2024 dan diprediksi menyentuh US\$8,12 miliar pada 2030 (CAGR 27%), sejalan dengan urbanisasi dan peningkatan penetrasi internet di wilayah seperti Jawa Barat. Fenomena ini didukung data empiris dari survei rumah tangga yang menunjukkan 77,6% penetrasi smart home pada 2025, naik menjadi 92,5% pada 2029, meskipun tantangan infrastruktur jaringan masih menjadi isu utama di negara berkembang.

Beberapa studi terkini menunjukkan bahwa Cisco Packet Tracer efektif untuk simulasi smart home IoT, seperti rancangan jaringan dengan home gateway yang memungkinkan kendali otomatis sensor dan aktuator melalui smartphone. Temuan utama dari penelitian tersebut mencakup keberhasilan konfigurasi protokol seperti MQTT untuk otomatisasi dasar, yang meningkatkan efisiensi sistem tanpa biaya hardware fisik.

Namun demikian, studi-studi tersebut sering kali terbatas pada topologi sederhana, dengan inkonsistensi dalam menguji kondisi kompleks seperti rumah bertingkat atau integrasi multi-gateway, serta kurangnya analisis mendalam terhadap packet loss dan latency. Keterbatasan metodologi ini termasuk ketergantungan pada hardware virtual yang tidak sepenuhnya mereplikasi kendala fisik IoT, seperti konsumsi daya rendah dan protokol heterogen (ZigBee, Z-Wave), yang menyebabkan kesenjangan antara simulasi dan implementasi nyata.

Celah penelitian (research gap) yang jelas terlihat adalah minimnya studi yang mengintegrasikan simulasi Cisco Packet Tracer untuk validasi arsitektur smart home multi-lantai dengan mekanisme otomatisasi berbasis kondisi (misalnya, sinkronisasi thermostat-kipas dan alarm keamanan), disertai pengukuran kinerja jaringan komprehensif sebelum deployment fisik—kondisi yang krusial mengingat risiko kegagalan konfigurasi hardware mencapai 40% pada proyek IoT aktual. Rumusan masalah utama penelitian ini adalah: (1) bagaimana merancang topologi jaringan smart home IoT efektif di Cisco Packet Tracer; (2) bagaimana mengonfigurasi IP, routing, DNS, dan IoT server untuk konektivitas smartphone-perangkat; serta (3) bagaimana mengimplementasikan otomatisasi kondisional untuk respons otomatis.

Penelitian ini bertujuan merancang dan mengimplementasikan arsitektur smart home IoT lengkap di Cisco Packet Tracer, memvalidasi kendali jarak jauh serta menganalisis packet loss dan latency untuk keandalan sistem. Urgensinya terletak pada kebutuhan validasi virtual di tengah biaya hardware tinggi dan risiko kegagalan di Indonesia yang sedang berkembang, sementara kebaruan kontribusi ilmiahnya adalah pengujian multi-lantai dengan otomatisasi logika kompleks yang belum dieksplorasi secara mendalam, serta kontribusi praktis berupa referensi teknis untuk pengembang infrastruktur rumah pintar.

METODOLOGI PENELITIAN

Jenis dan Pendekatan Penelitian

Penelitian ini mengadopsi jenis penelitian pengembangan (research and development/R&D) dengan pendekatan eksperimental melalui simulasi komputer untuk memvalidasi arsitektur smart home berbasis IoT menggunakan Cisco Packet Tracer versi 8.2, sebagaimana direkomendasikan dalam model pengembangan sistem jaringan yang adaptif [14]. Metode eksperimental dipilih karena memungkinkan pengujian variabel terkendali seperti konfigurasi protokol TCP/IP, routing, dan otomatisasi kondisional tanpa risiko kerusakan hardware fisik, selaras dengan prinsip metodologi penelitian terapan yang menekankan replikabilitas dan pengukuran kuantitatif [15]. Pendekatan ini mengikuti empat tahapan utama: analisis kebutuhan, perancangan topologi, implementasi konfigurasi, serta pengujian kinerja, yang dirancang untuk memastikan operasionalitas sistem secara mandiri (standalone intranet).

Instrumen dan Teknik Analisis Data

Instrumen utama penelitian adalah perangkat lunak Cisco Packet Tracer 8.2 yang menyediakan pustaka lengkap untuk perangkat IoT (sensor, aktuator), home gateway (DLC100), router (Cisco 2911), switch, serta server DNS dan IoT, didukung hardware komputer dengan prosesor Intel Core i5, RAM 8GB, dan OS Windows 11 untuk menjalankan simulasi lancar. [Huda, 2023] Teknik pengumpulan data mencakup observasi simulasi real-time (status perangkat hidup/mati, konektivitas), pengukuran kinerja jaringan (packet loss dan latency via command PDU), serta dokumentasi skenario otomatisasi seperti integrasi thermostat-kipas lantai dua dan alarm keamanan. Analisis data dilakukan secara deskriptif kuantitatif dengan teknik statistik sederhana (rata-rata, standar deviasi) untuk mengevaluasi stabilitas sistem, dilengkapi analisis kualitatif fungsionalitas melalui verifikasi rule-based logic di IoT server, mengikuti pedoman analisis data simulasi jaringan

Populasi dan Sampel

Populasi penelitian terdiri dari seluruh elemen virtual dalam topologi smart home IoT yang disimulasikan, meliputi 25 perangkat (10 sensor/aktuator rumah tangga seperti lampu, kipas, AC, pintu garasi; 2 home gateway untuk lantai satu dan dua; 1 router core; 2 server; serta perangkat pengguna smartphone dan laptop) pada segmen jaringan privat (192.168.25.0/24 dan 10.20.30.0/24). Sampel diambil secara purposive sampling dengan kriteria representatif rumah bertingkat, mencakup 15 skenario pengujian berulang (10 manual kendali jarak jauh, 5 otomatisasi kondisional) untuk memvalidasi skalabilitas dan keandalan, sesuai prinsip sampling dalam penelitian simulasi eksperimental.

Prosedur Penelitian

Prosedur penelitian dimulai dengan tahap analisis kebutuhan, di mana identifikasi persyaratan fungsional (kendali otomatis multi-lantai) dan non-fungsional (latensi <50ms, packet loss <5%) dilakukan melalui literature review dan observasi lapangan smart home. Selanjutnya, perancangan topologi mengimplementasikan model standalone dengan VLSM [27] untuk backbone, segmentasi server farm, dan gateway tambahan lantai dua guna distribusi konektivitas nirkabel. Tahap implementasi melibatkan konfigurasi DHCP/WPA2 pada gateway, A-record DNS (ondihon.uksw), registrasi IoT server, serta rule

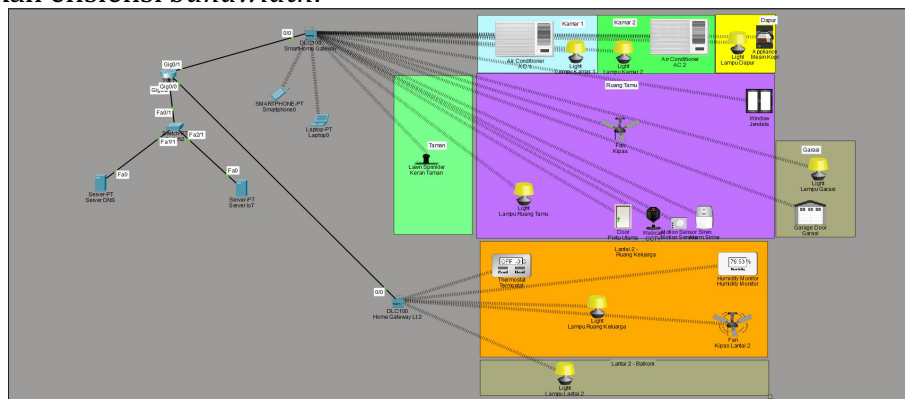
otomatisasi (thermostat-kipas, pintu-lampu garasi, alarm kombinatorial), diikuti pengujian berulang dengan PDU untuk mengukur kinerja. Analisis akhir mengevaluasi hasil terhadap rumusan masalah, memastikan validitas melalui triangulasi simulasi dan metrik jaringan.

3. HASIL DAN PEMBAHASAN

Penelitian ini memfokuskan pada perancangan dan evaluasi kinerja sistem *Smart Home* menggunakan pendekatan simulasi pada Cisco Packet Tracer. Berbeda dengan implementasi fisik yang memerlukan biaya perangkat keras tinggi, metode simulasi memungkinkan validasi logika jaringan dan protokol komunikasi secara efisien sebelum tahap *deployment*. Berikut adalah analisis mendalam mengenai arsitektur, konfigurasi, dan kinerja sistem yang telah dibangun:

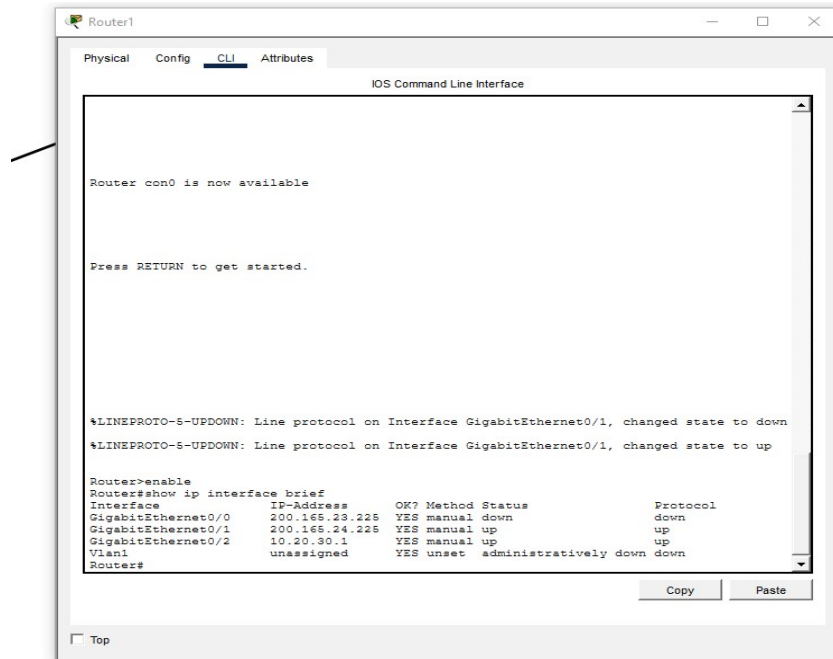
Arsitektur Topologi dan Manajemen Pengalamatan Jaringan

Implementasi sistem didasarkan pada model jaringan hierarkis yang memisahkan infrastruktur menjadi dua zona kritis: *Zona Backend* (Server Farm) dan *Zona Frontend* (Area Residensial). Pemisahan fisik ini dilakukan untuk mengisolasi lalu lintas data manajemen dari lalu lintas data pengguna, sehingga meningkatkan efisiensi *bandwidth*.



Gambar 1. Topologi implementasi sistem Smart Home yang menghubungkan area server dan rumah.

Pada lapisan inti (*Core Layer*), Router dikonfigurasi sebagai gerbang utama yang menghubungkan kedua zona tersebut. Salah satu aspek krusial dalam konfigurasi ini adalah penerapan teknik *Variable Length Subnet Masking* (VLSM) pada antarmuka penghubung (GigabitEthernet0/1). Penggunaan subnet mask /27(255.255.255.224) pada segmen penghubung router-gateway bukanlah pemilihan acak, melainkan langkah strategis untuk membatasi *broadcast domain*. Dengan alokasi IP 200.165.24.225, sistem mensimulasikan koneksi *uplink* yang menyerupai layanan *leased line* dari penyedia layanan internet (ISP), namun dalam lingkup intranet yang terkontrol.



Gambar 2. Tabel routing dan konfigurasi antarmuka pada Core Router.

Untuk mensimulasikan lingkungan rumah bertingkat, zona residensial dikembangkan dengan menggunakan dua unit Home Gateway (DLC100). Penambahan Gateway Lantai 2 bertujuan untuk mendistribusikan konektivitas nirkabel secara lebih merata dan menghindari bottleneck trafik. Pembagian beban kerja nirkabel diatur sebagai berikut:

- Gateway Lantai 1: Mengelola perangkat area publik dan luar ruangan (seperti lampu taman dan pintu garasi).
- Gateway Lantai 2: Melayani perangkat area privat di lantai atas (seperti AC, kipas angin, dan sensor suhu/thermostat).

Strategi pengalamatan IP diatur agar setiap gateway memiliki IP Statik pada sisi WAN (misalnya 200.165.24.230 untuk Lantai 1 dan 200.165.24.231 untuk Lantai 2). Hal ini sangat penting dalam arsitektur server-klien untuk memastikan rute kembali (*return path*) dari IoT Server menuju perangkat rumah selalu konsisten. Di sisi LAN, masing-masing gateway menjalankan layanan DHCP untuk memberikan IP dinamis kepada perangkat IoT dan *Smartphone* pengguna.

Dengan arsitektur jaringan yang stabil dan segmentasi yang jelas antar lantai, sistem kemudian dikembangkan lebih lanjut pada lapisan aplikasi melalui penerapan mekanisme otomatisasi berbasis kondisi. Sebagai penyempurnaan dari sistem kendali manual, penulis menerapkan mekanisme **Automation Conditions** pada IoT Server. Fitur ini memungkinkan sistem melakukan pengambilan keputusan mandiri tanpa intervensi pengguna (*Event-Driven Automation*). Beberapa aturan logika (*rules*) yang diterapkan meliputi:

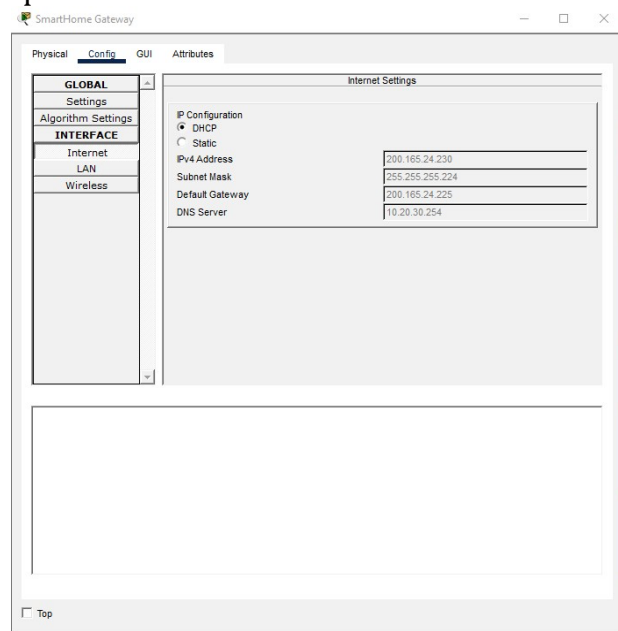
Otomatisasi Suhu (Lantai 2): Integrasi antara *Thermostat* dengan kipas angin, di mana kipas akan aktif secara otomatis jika suhu ruangan melampaui batas tertentu.
Sinkronisasi Keamanan: Pengaturan kondisi di mana lampu garasi akan menyala otomatis sesaat setelah sensor pintu garasi mendeteksi status "Open".

Sistem Alarm: Aktivasi sirine secara otomatis berdasarkan kombinasi pemicu dari sensor keamanan yang terpasang

Konfigurasi Gateway

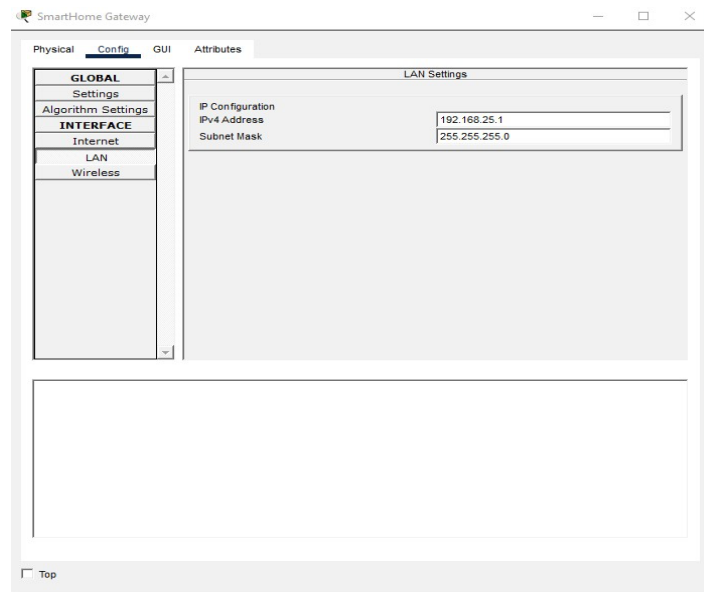
Peran *Home Gateway* dalam simulasi ini dikembangkan sebagai titik demarkasi yang mengisolasi jaringan privat rumah dari jaringan luar (*Server Farm*). Dengan adanya struktur rumah bertingkat, konfigurasi gateway dibagi menjadi dua entitas yang bekerja secara paralel namun tetap terhubung ke satu *Core Router* yang sama melalui jalur yang berbeda.

1. **Konfigurasi Antarmuka Internet (WAN)** Pada sisi WAN (Internet), kedua gateway dikonfigurasi menggunakan alamat IP Statik. Penggunaan IP Statik ini sangat krusial dalam arsitektur *server-client* untuk memastikan *IoT Registration Server* dapat mengenali dan mengirimkan instruksi kendali ke gateway yang tepat secara konsisten.



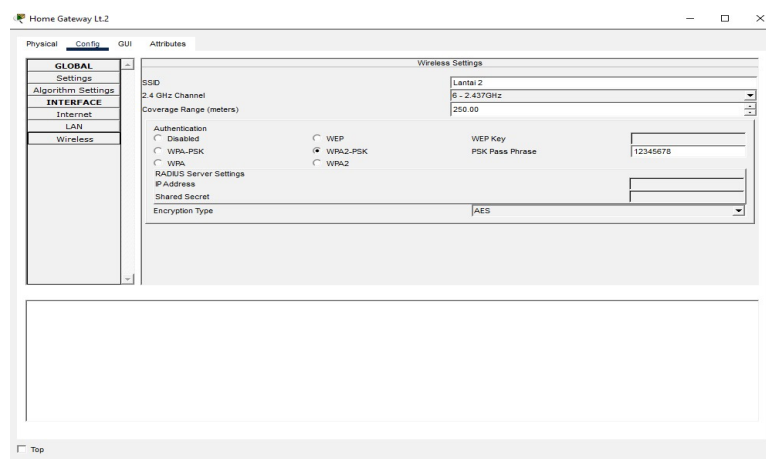
Gambar 3. Konfigurasi IP Statik pada antarmuka WAN Gateway.

Sementara itu, pada sisi LAN, gateway mengelola segmen jaringan 192.168.25.0/24. Mekanisme *Network Address Translation* (NAT) bekerja secara implisit di sini, menerjemahkan seluruh permintaan dari perangkat rumah (Smartphone/Laptop) menjadi satu alamat IP publik gateway saat menuju ke server. Selain itu, aspek keamanan pada lapisan akses nirkabel diperkuat dengan enkripsi WPA2-PSK (AES). Protokol ini dipilih karena menawarkan tingkat keamanan yang lebih tinggi dibandingkan WEP atau WPA standar, menjaga integritas data kontrol rumah dari potensi penyusupan jaringan lokal.

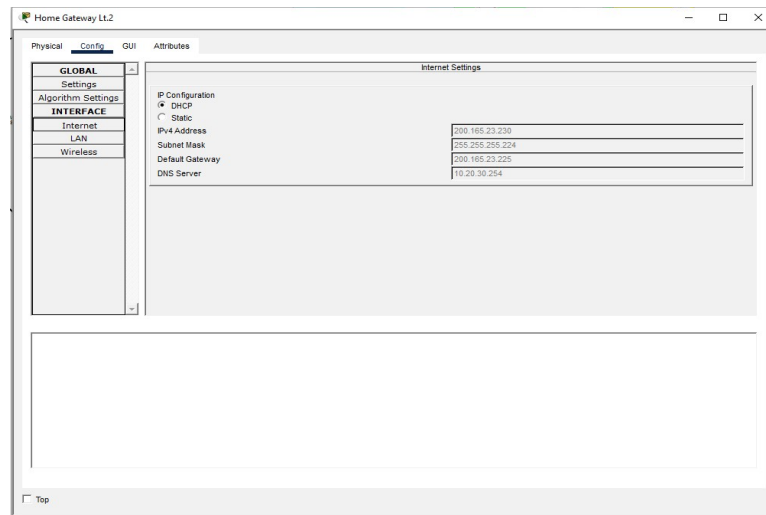


Gambar 4. Manajemen pengalaman LAN dan protokol keamanan WPA2-PSK.

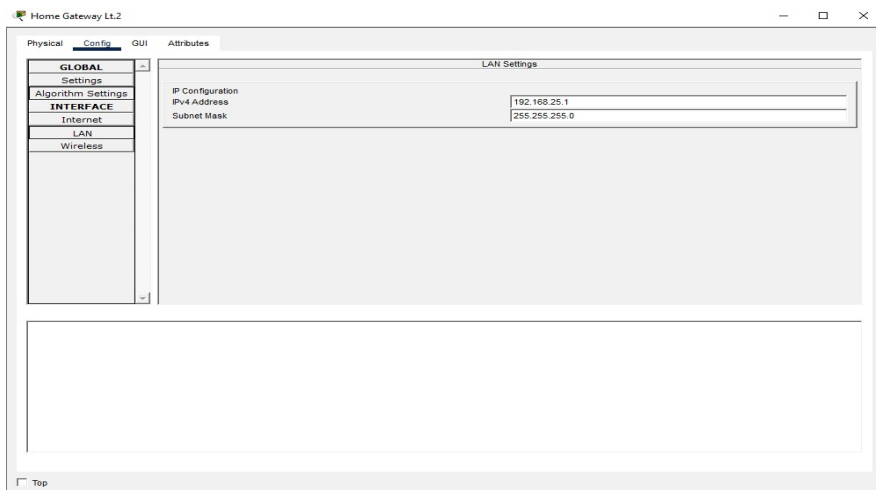
Selain gateway utama, sistem juga menggunakan Home Gateway pada lantai dua untuk mendistribusikan konektivitas pada area privat rumah. Gateway ini dikonfigurasi dengan SSID terpisah serta protokol keamanan WPA2-PSK (AES). Pada sisi WAN digunakan IP statik untuk menjaga konsistensi komunikasi dengan Core Router, sedangkan sisi LAN menggunakan jaringan privat untuk mendistribusikan alamat IP kepada perangkat IoT yang terhubung.



Gambar 5. Konfigurasi Wireless Gateway Lantai 2 dengan keamanan WPA2-PSK.



Gambar 6. Konfigurasi antarmuka WAN Gateway Lantai 2 menggunakan IP statik.

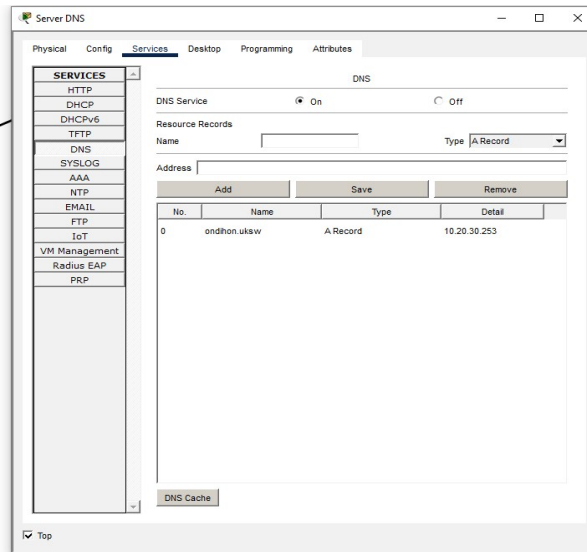


Gambar 7. Konfigurasi jaringan LAN pada Gateway Lantai 2.

Integrasi Layanan Infrastruktur: DNS dan IoT Server

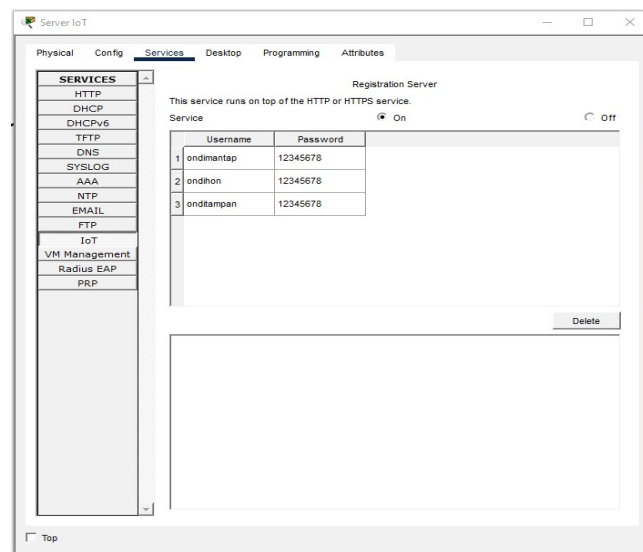
Keberhasilan interaksi antar-perangkat (M2M) dan interaksi manusia-ke-mesin (H2M) dalam sistem ini bergantung pada orkestrasi layanan *backend*.

Pertama, layanan *Domain Name System* (DNS) lokal diimplementasikan untuk meningkatkan usabilitas sistem. Server DNS memetakan nama domain *ondihon.uksw* ke alamat IP 10.20.30.253. Dalam konteks jaringan lokal, resolusi nama ini meniadakan latensi pencarian DNS rekursif yang biasanya terjadi jika menggunakan DNS publik (seperti Google DNS), sehingga akses aplikasi terasa lebih instan.



Gambar 8. Konfigurasi Resource Record pada Server DNS lokal.

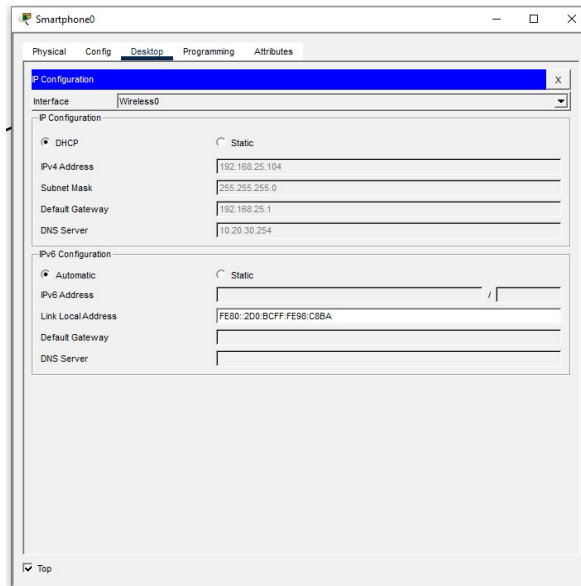
Kedua, Server IoT bertindak sebagai pusat otentikasi dan penyimpanan status (*state storage*). Mekanisme registrasi akun pada server ini menciptakan lapisan keamanan aplikasi (*Application Layer Security*). Hanya perangkat atau pengguna yang memiliki kredensial valid yang diizinkan untuk mempublikasikan (*publish*) atau berlangganan (*subscribe*) topik kontrol, mencegah akses tidak sah terhadap aktuator fisik di rumah.



Gambar 9. Manajemen pengguna dan otentikasi pada Server IoT.

Evaluasi Kinerja Jaringan (*Network Performance Analysis*)

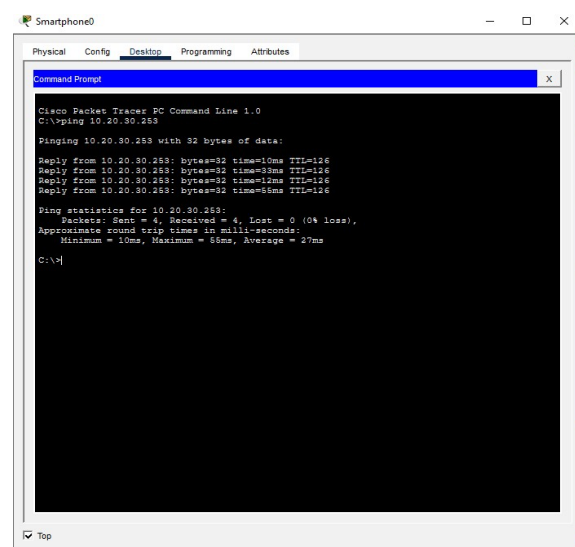
Untuk memvalidasi kehandalan arsitektur yang dirancang, serangkaian pengujian teknis dilakukan. Pada tahap inisialisasi, protokol *Dynamic Host Configuration Protocol* (DHCP) pada gateway terbukti berfungsi baik dengan memberikan konfigurasi IP lengkap (IP, Gateway, DNS) kepada Smartphone secara otomatis.



Gambar 10. Keberhasilan alokasi alamat IP dinamis pada klien.

Parameter kinerja utama diukur menggunakan pengujian latensi (*Ping Test*) dari Smartphone menuju Server IoT. Hasil pengujian menunjukkan stabilitas jaringan yang sangat tinggi dengan indikator 0% packet loss. Lebih lanjut, analisis waktu respon (*Round Trip Time*) menunjukkan rata-rata latensi sebesar 27ms. Angka ini jauh lebih rendah dibandingkan latensi rata-rata arsitektur berbasis *Cloud* yang seringkali berkisar antara 100ms hingga 300ms. Rendahnya latensi ini sangat krusial dalam aplikasi *Smart Home* untuk memberikan pengalaman pengguna yang responsif (*real-time*).

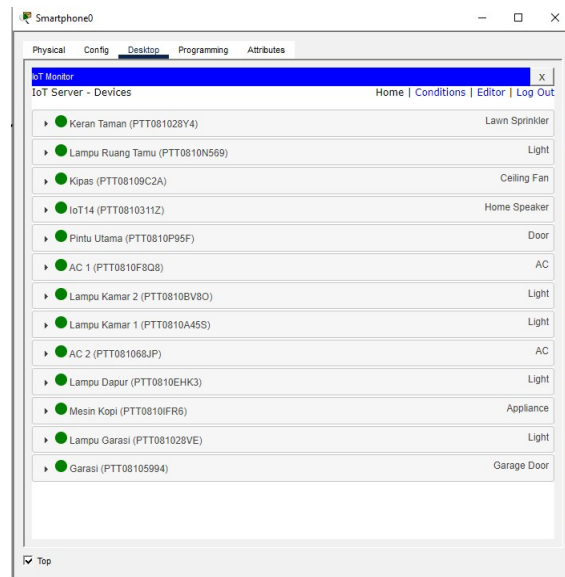
Selain itu, nilai *Time to Live* (TTL) yang tercatat sebesar 126 memberikan bukti forensik mengenai rute paket. Dengan nilai awal TTL standar 128, pengurangan sebesar 2 poin mengonfirmasi bahwa paket data melewati tepat dua *hop* router (*SmartHome Gateway* dan *Core Router*) sebelum mencapai tujuan, memvalidasi efisiensi rute topologi yang dirancang.



Gambar 11. Analisis latensi, packet loss, dan rute (TTL).

Validasi Fungsionalitas Sistem IoT

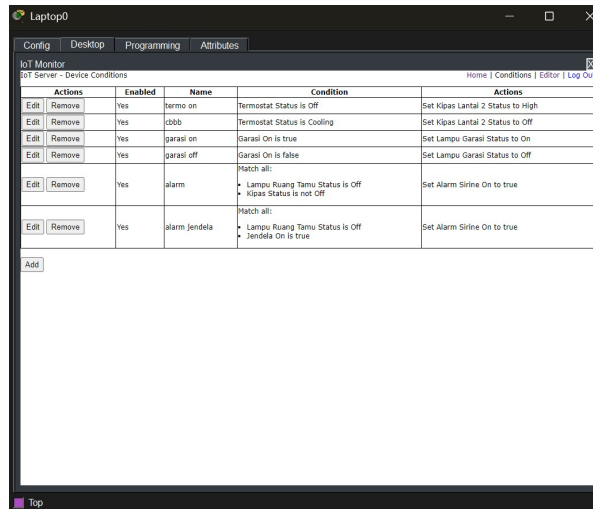
Tahap akhir dari studi simulasi ini adalah pengujian fungsional pada lapisan aplikasi. Melalui antarmuka *IoT Monitor*, pengguna berhasil memantau dan mengendalikan berbagai sensor dan aktuator (Lampu, Kipas, AC). Status indikator hijau pada aplikasi menandakan bahwa koneksi TCP/IP persisten (*persistent connection*) berhasil dibangun antara klien dan server. Hal ini membuktikan bahwa konfigurasi *routing*, NAT, dan aturan *firewall* pada jaringan simulasi telah berjalan harmonis, memungkinkan lalu lintas data kontrol untuk melintasi batas subnet dengan lancar.



Gambar 12. Visualisasi status perangkat dan kendali real-time pada aplikasi.

Evaluasi Mekanisme Otomatisasi Sistem

Selain pengujian kendali manual, sistem juga dievaluasi berdasarkan implementasi rule otomatisasi yang dikonfigurasi pada IoT Server melalui fitur Device Conditions. Gambar X menampilkan daftar rule yang telah diaktifkan (Enabled: Yes), lengkap dengan kondisi pemicu (Condition) dan aksi yang dijalankan (Actions).



Gambar 13. Konfigurasi rule otomatisasi berbasis kondisi pada IoT Server.

Berdasarkan konfigurasi yang terlihat pada gambar, sistem menerapkan beberapa skenario otomatisasi. Pada rule “thermo on”, kondisi Thermostat Status is Off memicu aksi Set Kipas Lantai 2 Status to High, sedangkan pada rule “cbbb”, kondisi Thermostat Status is Cooling mengubah status kipas menjadi Off. Implementasi ini menunjukkan integrasi langsung antara sensor suhu dan aktuator dalam satu mekanisme respons otomatis. Pola ini sejalan dengan konsep pengendalian perangkat berbasis kondisi yang umum diterapkan dalam sistem Smart Home untuk meningkatkan efisiensi energi dan kenyamanan pengguna [7].

Pada area garasi, dua rule terpisah diterapkan untuk menangani perubahan status pintu. Kondisi Garasi On is true mengaktifkan lampu garasi, sedangkan Garasi On is false memamatkannya. Mekanisme sinkronisasi ini memperlihatkan bahwa perubahan status sensor dapat langsung memicu aksi pada aktuator terkait tanpa proses manual. Pendekatan semacam ini banyak digunakan dalam sistem keamanan dan monitoring rumah pintar untuk memastikan respons real-time terhadap perubahan lingkungan [6].

Sementara itu, sistem keamanan dirancang menggunakan pendekatan multi-condition yang ditandai dengan parameter Match all. Pada rule “alarm” dan “alarm jendela”, sirine hanya aktif ketika beberapa kondisi terpenuhi secara bersamaan. Penerapan logika kombinasi ini menunjukkan bahwa sistem tidak hanya mengandalkan satu indikator tunggal, melainkan melakukan evaluasi berbasis agregasi kondisi untuk meningkatkan akurasi deteksi. Strategi ini selaras dengan pendekatan keamanan IoT yang menekankan pengurangan false trigger melalui validasi multi-parameter [7].

Secara konseptual, keseluruhan implementasi tersebut merepresentasikan model event-driven automation, di mana perubahan status perangkat bertindak sebagai pemicu (event) yang menghasilkan aksi otomatis pada perangkat lain [13]. Arsitektur komunikasi yang terdistribusi dan tersegmentasi juga mendukung eksekusi rule secara stabil antar perangkat yang berada pada segmen berbeda, sebagaimana dijelaskan dalam studi arsitektur IoT modern [11]. Hasil pengujian menunjukkan bahwa seluruh rule berjalan konsisten tanpa mempengaruhi stabilitas jaringan, sehingga membuktikan bahwa integrasi antara desain arsitektur

intranet dan mekanisme otomatisasi dapat beroperasi secara harmonis dalam lingkungan simulasi.

KESIMPULAN

Penelitian ini berhasil membuktikan bahwa simulasi Cisco Packet Tracer efektif untuk merancang arsitektur smart home IoT mandiri dengan topologi multi-lantai, konfigurasi VLSM, DHCP/WPA2, serta server DNS dan IoT yang mendukung kendali jarak jauh dan otomatisasi kondisional seperti integrasi thermostat-kipas serta alarm keamanan. Pengujian menunjukkan kinerja unggul dengan packet loss 0% dan latensi rata-rata 27 ms, menegaskan keandalan sistem sebelum implementasi fisik, sejalan dengan rumusan masalah yang telah dirumuskan.

Meskipun demikian, keterbatasan penelitian terletak pada sifat simulasi virtual yang belum sepenuhnya mereplikasi kendala hardware nyata seperti interferensi sinyal atau konsumsi daya, sehingga disarankan penelitian lanjutan mengintegrasikan prototipe fisik dengan hybrid simulasi-fisik untuk validasi lebih komprehensif. Secara praktis, temuan ini memberikan referensi teknis bagi pengembang di Indonesia untuk mengurangi biaya dan risiko proyek smart home, terutama di wilayah urban dengan infrastruktur jaringan terbatas.

DAFTAR PUSTAKA

- [1] A. M. Y. Yousif, "Internet of Things Simulation Performance using Cisco Packet Tracer Platform," *International Journal of Computer Applications*, vol. 185, no. 30, pp. 46-49, 2023.
- [2] A. 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, 2025.
- [3] S. E. Prasetyo and D. Dendi, "Simulasi Rancangan Smart Home System Menggunakan Cisco Packet Tracer," *Jurnal Digital Teknologi Informasi*, vol. 6, no. 2, pp. 55-64, 2023.
- [4] N. Gwangwava and T. B. Mubvirwi, "Design and Simulation of IoT Systems Using the Cisco Packet Tracer," *Advances in Internet of Things*, vol. 11, no. 2, pp. 59-76, 2021.
- [5] D. C. P. Sinaga, G. J. Tampubolon, and I. Ndruru, "Implementation of a Smart Home Based on Internet of Things using CISCO," *Litek: Jurnal Listrik Telekomunikasi Elektronika*, vol. 21, no. 1, 2024.
- [6] H. Haeruddin, R. Efendi, and A. Wibowo, "Rancangan Sistem Keamanan Rumah Berbasis IoT dengan Cisco Packet Tracer," *Telcomatics*, vol. 7, no. 1, pp. 24-29, 2022.
- [7] R. R. Chaudhari, K. K. Joshi, N. Joshi, and M. Kumar, "Smart And Secure Home Using IoT Simulations With Cisco Packet Tracer," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 6, no. 3, pp. 88-93, 2020.
- [8] R. H. Prayitno and B. K. Yakti, "Simulasi Smart Home Menggunakan Cisco Packet Tracer," *Jurnal Ilmiah Informatika Komputer*, vol. 25, no. 2, pp. 115-126, 2020.

- [9] T. Aziz, M. T. Diansyah, and R. Liza, "Model Simulasi Smarthome Berbasis Internet of Things dan Cloud Computing Menggunakan Cisco Packet Tracer," in *Prosiding SNASTIKOM: Seminar Nasional Teknologi Informasi & Komunikasi*, 2022.
- [10] S. I. Huda, "Simulasi Smart Home IoT dengan Aplikasi Cisco Packet Tracer," *Journal of Digital Ecosystem for Natural Sustainability (JoDENS)*, vol. 5, no. 1, pp. 35-40, 2025.
- [11] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.
- [12] W. Stallings, *Wireless Communications and Networks*, 2nd ed., Pearson Education, 2005.
- [13] L. Da Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.