Madani: Jurnal Ilmiah Multidisiplin
Volume 4, Nomor 9, October 2026, P. 21-27
E-ISSN: 2986-6340
Licenced by CC BY-SA 4.0
DOI: https://doi.org/10.5281/zenodo.23260251

Perancangan dan Implementasi Jaringan *Wireless Huawei* Berbasis WLC Menggunakan Multi VLAN dan *MAC Address Filtering* Pada PT Xyz

Design and Implementation of a Huawei WLC-Based Wireless Network Using Multiple VLANs and MAC Address Filtering at PT XYZ

Lindra Mahesa Putra[1*], **Firmansyah**[2]
[1,2]Program Studi Teknologi Informasi, Universitas Bina Sarana Informatika, Jakarta, Indonesia
Email*: 17220415@bsi.ac.id, firmansyah.fmy@bsi.ac.id

ABSTRAK

Infrastruktur jaringan wireless pada lingkungan enterprise memerlukan sistem manajemen yang terpusat, terstruktur, dan aman. Penelitian ini bertujuan merancang dan mengimplementasikan jaringan wireless berbasis Wireless LAN Controller (WLC) Huawei menggunakan Multi VLAN dan MAC Address Filtering pada simulator Huawei eNSP dengan studi kasus di PT XYZ. Permasalahan yang ditemukan meliputi belum adanya segmentasi jaringan wireless berdasarkan kategori pengguna, belum diterapkannya MAC Address Filtering pada jaringan khusus Direktur Utama, serta pengelolaan Access Point yang masih dilakukan secara standalone tanpa manajemen terpusat. Metode penelitian yang digunakan adalah Network Development Life Cycle (NDLC) yang terdiri dari enam tahapan, yaitu Analysis, Design, Simulation Prototype, Implementation, Monitoring, dan Management. Jaringan dirancang menggunakan topologi hierarki tiga tingkat dengan komponen Router Huawei AR2220, Switch Agregasi Huawei S5720, Switch Access PoE Huawei S3700, WLC Huawei AC6005/AC6605, dan tiga unit Access Point yang seluruhnya disimulasikan pada Huawei eNSP V100R003C00. Hasil implementasi menunjukkan bahwa seluruh tiga unit Access Point berhasil terdaftar ke WLC secara otomatis melalui protokol CAPWAP (RFC 5415 dan RFC 5416) [7]. Segmentasi jaringan berhasil diterapkan dengan empat VLAN, yaitu VLAN 10 (Tamu), VLAN 20 (Staff), VLAN 30 (Direktur Utama), dan VLAN 100 (Manajemen). MAC Address Filtering berbasis whitelist berhasil membatasi koneksi VLAN Direktur Utama hanya kepada dua perangkat terdaftar. DHCP lease time berhasil dikonfigurasi berbeda pada tiap VLAN, ACL nomor 3100 berhasil mengisolasi traffic antar VLAN pengguna, dan fitur Fast BSS Transition (802.11r) memungkinkan roaming otomatis perangkat Direktur Utama antara SSID 2,4 GHz dan 5 GHz tanpa autentikasi ulang.
Kata kunci: CAPWAP, eNSP, jaringan enterprise, MAC address filtering, multi VLAN, WLC Huawei

ABSTRACT

Wireless network infrastructure in an enterprise environment requires a centralized, structured, and secure management system. This research aims to design and implement a wireless network based on a Huawei Wireless LAN Controller (WLC) using Multi VLAN and MAC Address Filtering on the Huawei eNSP simulator, with a case study at PT XYZ. The problems identified include the absence of wireless network segmentation based on user categories, the lack of MAC Address Filtering on the Director's dedicated network, and Access Point management still being done in standalone mode without a centralized management system. The research method used is the Network Development Life Cycle (NDLC), consisting of six stages: Analysis, Design, Simulation Prototype, Implementation, Monitoring, and Management. The results show that all three Access Points successfully registered to the WLC automatically via the CAPWAP protocol (RFC 5415 and RFC 5416). Network segmentation was successfully implemented with four VLANs. MAC Address Filtering successfully restricted the Director's VLAN connection to only two registered devices. DHCP lease time was configured differently per VLAN, ACL number 3100 successfully isolated inter-VLAN traffic, and Fast BSS Transition (802.11r) enabled automatic roaming between the 2.4 GHz and 5 GHz SSIDs for the Director without re-authentication.
Keywords: CAPWAP, enterprise network, eNSP, Huawei WLC, MAC address filtering, multi VLAN

Article Info
Received date: 22 September 2026 Revised date: 30 September 2026 Accepted date:07 October 2026

PENDAHULUAN

Perkembangan teknologi jaringan nirkabel dalam beberapa tahun terakhir mengalami pertumbuhan yang sangat pesat seiring dengan meningkatnya kebutuhan konektivitas di berbagai sektor organisasi. Kebutuhan akan infrastruktur jaringan yang andal, aman, dan mudah dikelola mendorong

adopsi teknologi Wireless LAN Controller (WLC) sebagai solusi manajemen jaringan nirkabel terpusat. Penggunaan sistem controller memungkinkan administrator jaringan melakukan konfigurasi, monitoring, dan pemeliharaan banyak Access Point dari satu titik kendali secara efisien [1]. WLC menjadi semakin relevan ketika sebuah organisasi memiliki banyak pengguna dengan kebutuhan akses berbeda-beda, seperti staff, tamu, dan manajemen puncak [2].

Dalam lingkungan jaringan enterprise, segmentasi jaringan menggunakan Virtual Local Area Network (VLAN) merupakan praktik terbaik untuk membatasi ruang lingkup broadcast, meningkatkan keamanan, dan memudahkan pengelolaan kebijakan akses [3]. Implementasi VLAN terbukti mampu memisahkan jaringan menjadi beberapa sub-jaringan yang terisolasi secara logis sehingga pengelolaan bandwidth dan keamanan jaringan menjadi lebih optimal [4]. Permasalahan yang umum dijumpai di lapangan adalah belum optimalnya manajemen jaringan nirkabel, di mana seluruh pengguna masih berada dalam satu segmen jaringan yang sama tanpa pemisahan antara pengguna biasa, tamu, dan pimpinan, sehingga menimbulkan risiko keamanan berupa akses tidak sah terhadap sumber daya jaringan.

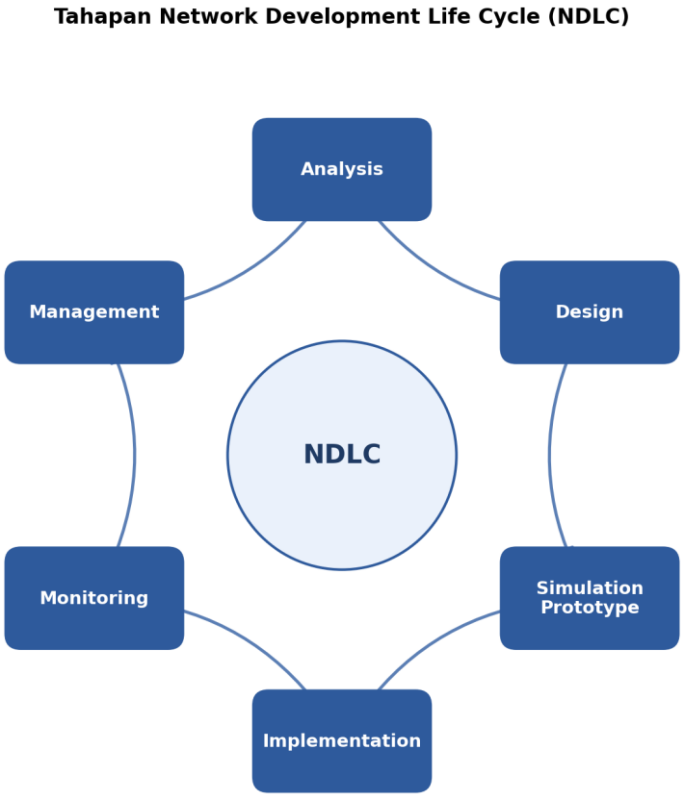
Aspek keamanan tambahan yang juga penting dalam jaringan wireless enterprise adalah penerapan MAC Address Filtering, yaitu mekanisme yang membatasi akses hanya kepada perangkat yang telah terdaftar. Penggabungan MAC Address Filtering dengan WPA2-PSK terbukti efektif memblokir pengguna tidak berwenang meskipun mereka telah mengetahui password SSID [5]. Berdasarkan permasalahan tersebut, penelitian ini merancang dan mengimplementasikan WLC Huawei pada simulator eNSP dengan empat VLAN, yaitu VLAN 10 untuk Tamu, VLAN 20 untuk Staff, VLAN 30 untuk Direktur Utama, serta VLAN 100 sebagai jaringan manajemen WLC dan Access Point, yang dilengkapi dengan MAC Address Filtering berbasis whitelist pada VLAN Direktur Utama.

Rumusan masalah pada penelitian ini adalah: (1) bagaimana merancang dan mengimplementasikan jaringan wireless berbasis WLC Huawei pada simulator eNSP; (2) bagaimana menerapkan segmentasi jaringan menggunakan Multi VLAN pada WLC Huawei; (3) bagaimana mengimplementasikan MAC Address Filtering pada VLAN Direktur Utama; dan (4) bagaimana memastikan distribusi IP Address kepada klien pada masing-masing VLAN berjalan dengan baik melalui DHCP Server. Tujuan penelitian ini adalah merancang dan mengimplementasikan konfigurasi WLC Huawei dengan segmentasi Multi VLAN, kontrol akses MAC Address Filtering, serta memvalidasi fungsionalitas konfigurasi melalui pengujian konektivitas, distribusi DHCP, pembatasan akses antar VLAN menggunakan Access Control List (ACL), dan kebijakan MAC Address Filtering.

METODE

Penelitian ini menggunakan metode Network Development Life Cycle (NDLC), yaitu model yang menjelaskan rangkaian tahapan dalam proses perancangan, pembangunan, dan pengembangan sistem jaringan komputer secara berkesinambungan [6]. NDLC dipilih karena memiliki tahapan yang sistematis mulai dari analisis kebutuhan hingga pengelolaan jaringan. Tahapan NDLC yang diterapkan pada penelitian ini terdiri dari enam tahap sebagai berikut.

1. *Analysis*: mengidentifikasi kebutuhan jaringan, permasalahan pada jaringan berjalan, kebutuhan segmentasi VLAN, serta perangkat jaringan yang digunakan.
2. *Design*: membuat rancangan topologi jaringan wireless berbasis WLC Huawei dan Multi VLAN menggunakan simulator eNSP.
3. *Simulation Prototype*: mengimplementasikan konfigurasi jaringan pada Huawei eNSP untuk menguji rancangan yang telah dibuat.
4. *Implementation*: menerapkan konfigurasi WLC Huawei, Multi VLAN, MAC Address Filtering, dan ACL pada jaringan wireless.
5. *Monitoring*: menguji konektivitas jaringan antar VLAN, distribusi DHCP, MAC Address Filtering, dan pembatasan akses antar VLAN.
6. *Management*: mengelola dan mengevaluasi jaringan agar implementasi berjalan optimal dan stabil.



Gambar 1. Tahapan Network Development Life Cycle (NDLC)

Pengumpulan data dilakukan melalui dua teknik, yaitu observasi langsung terhadap jaringan yang berjalan di PT XYZ untuk mengetahui kebutuhan perangkat, topologi, dan permasalahan jaringan, serta studi pustaka terhadap buku, jurnal ilmiah, dan dokumentasi resmi mengenai Wireless LAN, WLC Huawei, VLAN, MAC Address Filtering, CAPWAP, DHCP, dan simulator eNSP. Perancangan dan pengujian jaringan dilakukan sepenuhnya pada simulator Huawei eNSP V100R003C00 [8], yang mendukung konfigurasi perangkat Huawei secara akurat, meliputi Router AR2220, Switch Agregasi S5720, Switch Access PoE S3700, WLC AC6005/AC6605, dan Access Point AP6050DN. Topologi yang digunakan adalah topologi hierarki tiga tingkat yang terdiri dari Core Layer (Router), Distribution Layer (Switch Agregasi), dan Access Layer (Switch Access PoE), yang merupakan standar desain jaringan enterprise modern [3].

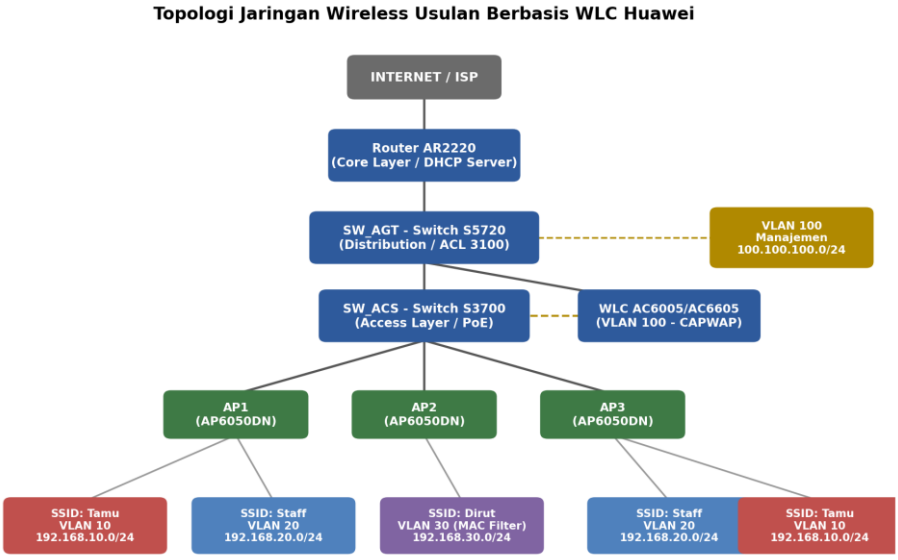
Segmentasi jaringan dirancang menggunakan empat VLAN, yaitu VLAN 10 (Tamu, 192.168.10.0/24), VLAN 20 (Staff, 192.168.20.0/24), VLAN 30 (Direktur Utama, 192.168.30.0/24), dan VLAN 100 (Manajemen, 100.100.100.0/24). Keamanan VLAN Direktur Utama diperkuat dengan MAC Address Filtering berbasis whitelist menggunakan fitur sta-whitelist-profile pada WLC Huawei, sedangkan isolasi antar VLAN pengguna diterapkan menggunakan Access Control List (ACL) nomor 3100 pada Switch Agregasi [9]. Pengujian dilakukan menggunakan perintah ping dan verifikasi CLI Huawei VRP untuk memastikan konektivitas, distribusi DHCP, isolasi ACL, dan efektivitas MAC Address Filtering berjalan sesuai rancangan.

HASIL DAN PEMBAHASAN

Topologi dan Segmentasi VLAN

Jaringan usulan dirancang dengan mengubah arsitektur wireless standalone menjadi arsitektur berbasis WLC Huawei AC6005/AC6605 yang mengelola tiga unit Access Point Huawei AP6050DN melalui protokol CAPWAP. Router Huawei AR2220 berfungsi sebagai Core Layer sekaligus DHCP

Server, Switch Agregasi Huawei S5720 berperan sebagai Distribution Layer yang menjalankan inter-VLAN routing dan ACL, sedangkan Switch Access PoE Huawei S3700 berfungsi sebagai Access Layer yang menyalurkan daya listrik ke Access Point. Topologi jaringan usulan secara lengkap ditunjukkan pada Gambar 2, sedangkan rancangan segmentasi Multi VLAN yang diterapkan ditunjukkan pada Tabel 1.



Gambar 2. Topologi Jaringan Wireless Usulan Berbasis WLC Huawei

Tabel 1. Rancangan segmentasi Multi VLAN

VLAN	Nama	Network Address	Fungsi
10	Tamu	192.168.10.0/24	Akses internet, tanpa akses resource internal.
20	Staff	192.168.20.0/24	Akses penuh ke resource internal.
30	Direktur Utama	192.168.30.0/24	Keamanan tertinggi dengan MAC Address Filtering.
100	Manajemen	100.100.100.0/24	Manajemen WLC dan AP, tertutup bagi pengguna umum.

Proses registrasi Access Point ke WLC berlangsung melalui protokol Control and Provisioning of Wireless Access Points (CAPWAP) yang didefinisikan pada RFC 5415 dan RFC 5416 [7]. Access Point memperoleh alamat IP dari VLAN 100 beserta DHCP Option 43 sub-option 2 yang berisi alamat WLC, kemudian mengirimkan CAPWAP Join Request yang direspons dengan CAPWAP Join Response oleh WLC. Hasil pengujian registrasi menunjukkan seluruh tiga unit Access Point berhasil terdaftar secara otomatis pada AP Group tanpa memerlukan konfigurasi manual satu per satu, sebagaimana ditunjukkan pada Tabel 2.

Tabel 2. Hasil pengujian registrasi Access Point ke WLC

Access Point	IP Address (DHCP WLC)	Status CAPWAP	Hasil

AP1	100.100.100.10/24	Run (Terdaftar)	Berhasil
AP2	100.100.100.11/24	Run (Terdaftar)	Berhasil
AP3	100.100.100.12/24	Run (Terdaftar)	Berhasil

MAC Address Filtering pada VLAN Direktur Utama

MAC Address Filtering diterapkan menggunakan fitur sta-whitelist-profile pada WLC Huawei untuk SSID VLAN Direktur Utama. Konfigurasi dilakukan dengan membuat whitelist profile, menambahkan MAC Address perangkat yang diizinkan, kemudian menerapkan profile tersebut pada VAP Profile SSID Direktur. Mekanisme ini terbukti efektif karena memverifikasi identitas perangkat di luar autentikasi WPA2-PSK, sehingga perangkat yang tidak terdaftar tetap ditolak meskipun mengetahui password SSID yang benar [5], [10]. Hasil pengujian menunjukkan bahwa hanya dua perangkat terdaftar yang berhasil terhubung, sedangkan perangkat lain yang tidak terdaftar ditolak oleh WLC, sebagaimana ditunjukkan pada Tabel 3.

Tabel 3. Hasil pengujian MAC Address Filtering pada VLAN 30

Perangkat	SSID	Status Whitelist	Hasil Koneksi
Laptop Direktur Utama	Dirut	Terdaftar	Berhasil
Smartphone Direktur Utama	Dirut	Terdaftar	Berhasil
Laptop Tamu (tidak dikenal)	Dirut	Tidak Terdaftar	Ditolak
Laptop Staff (tidak dikenal)	Dirut	Tidak Terdaftar	Ditolak

Konfigurasi DHCP Lease Time dan ACL Antar VLAN

Distribusi IP Address dilakukan oleh Router sebagai DHCP Server dengan lease time yang berbeda pada setiap VLAN untuk mengoptimalkan pengelolaan pool IP, mengacu pada mekanisme DORA (Discover, Offer, Request, Acknowledge) [6]. VLAN 10 (Tamu) dikonfigurasi dengan lease time 8 jam, VLAN 20 (Staff) 12 jam, dan VLAN 30 (Direktur Utama) tidak terbatas agar koneksi tidak terputus. Sementara itu, Access Control List (ACL) nomor 3100 diterapkan pada Switch Agregasi untuk mengisolasi VLAN Tamu, dengan mengacu pada penelitian yang membuktikan bahwa ACL secara efektif membatasi akses antar VLAN sehingga keamanan jaringan meningkat signifikan [11]. Hasil pengujian konektivitas antar VLAN ditunjukkan pada Tabel 4.

Tabel 4. Hasil pengujian ping antar VLAN setelah implementasi

Sumber	Tujuan	Hasil	Keterangan
VLAN 10 (Tamu)	VLAN 20 (Staff)	Gagal	Diblokir ACL 3100
VLAN 10 (Tamu)	VLAN 30 (Dirut)	Gagal	Diblokir ACL 3100
VLAN 10 (Tamu)	Internet (8.8.8.8)	Berhasil	Akses internet tersedia
VLAN 20 (Staff)	VLAN 30 (Dirut)	Berhasil	Tidak diblokir ACL

Perbandingan Sebelum dan Sesudah Implementasi

Perbandingan kondisi jaringan sebelum dan sesudah implementasi menunjukkan peningkatan yang signifikan pada seluruh aspek yang diukur. Sebelum implementasi, seluruh pengguna berada pada satu flat network tanpa segmentasi, Access Point dikelola secara standalone, dan tidak terdapat MAC Address Filtering maupun ACL. Setelah implementasi, jaringan terbagi menjadi empat VLAN yang terisolasi, Access Point dikelola secara terpusat melalui WLC, akses VLAN Tamu ke VLAN lain

diblokir oleh ACL, dan VLAN Direktur Utama dilindungi oleh MAC Address Filtering berbasis whitelist. Selain itu, fitur dual-band SSID dikonfigurasi untuk setiap kelompok pengguna, dan fitur Fast BSS Transition (802.11r) memungkinkan perangkat Direktur Utama berpindah dari SSID 2,4 GHz ke SSID 5 GHz secara otomatis tanpa autentikasi ulang, sehingga meningkatkan kenyamanan sekaligus keamanan pengguna dengan hak akses tertinggi.

SIMPULAN

Berdasarkan hasil perancangan, implementasi, dan pengujian yang telah dilakukan, dapat disimpulkan bahwa jaringan wireless berbasis WLC Huawei AC6005/AC6605 berhasil diimplementasikan pada simulator Huawei eNSP, dengan seluruh tiga unit Access Point berhasil terdaftar secara otomatis melalui protokol CAPWAP tanpa konfigurasi manual. Segmentasi Multi VLAN berhasil membagi jaringan menjadi empat segmen yang terisolasi, MAC Address Filtering berbasis whitelist berhasil membatasi akses VLAN Direktur Utama hanya kepada perangkat terdaftar, konfigurasi DHCP lease time berhasil disesuaikan dengan kebutuhan setiap kelompok pengguna, dan ACL nomor 3100 berhasil mengisolasi VLAN Tamu dari VLAN pengguna lainnya. Seluruh hasil pengujian konektivitas membuktikan bahwa konfigurasi jaringan berfungsi sesuai dengan rancangan yang diusulkan.

Penelitian selanjutnya disarankan untuk mengintegrasikan autentikasi RADIUS Server (802.1X EAP-TLS) guna menggantikan WPA2-PSK dengan kredensial pengguna yang unik, menerapkan Quality of Service (QoS) untuk membatasi bandwidth per VLAN, serta menambahkan WLC kedua sebagai redundansi untuk meningkatkan ketersediaan jaringan. Selain itu, pengujian pada perangkat Huawei fisik diperlukan untuk memverifikasi kompatibilitas dan performa konfigurasi dalam kondisi operasional sebenarnya, serta perbandingan dengan controller berbasis merek lain seperti Cisco atau Aruba dapat menjadi topik penelitian lanjutan yang relevan.

REFERENSI

[1] M. A. Faizi and F. W. Christanto, “Manajemen perangkat jaringan Access Point menggunakan UniFi Controller di jaringan kampus,” JUSTINDO, vol. 9, no. 2, pp. 67–76, 2024, doi: 10.32528/justindo.v9i2.1471.

[2] B. A. Forouzan, Data Communications and Networking with TCP/IP Protocol Suite. New York, NY, USA: McGraw-Hill, 2022.

[3] J. F. Kurose and K. W. Ross, Computer Networks: A Top-Down Approach, 8th ed. London, UK: Pearson, 2022.

[4] Novinaldi, R. Nurbahri, and Ikhsan, “Perancangan dan implementasi Virtual Local Area Network (VLAN) untuk optimalisasi bandwidth jaringan: Studi kasus Universitas Baiturrahmah,” Jurnal Pustaka Data, vol. 1, no. 1, pp. 13–18, 2021.

[5] Firmansyah, R. A. Purnama, and R. D. Astuti, “Optimalisasi keamanan wireless menggunakan filtering MAC address,” Keilmuan dan Aplikasi Bidang Teknik Informatika, vol. 15, no. 1, pp. 25–33, 2021.

[6] S. Hotmariana and Y. Syafitri, “Analisis dan perancangan infrastruktur jaringan komputer menggunakan metode NDLC (Network Development Life Cycle) studi kasus: SMP Negeri 34 Bandar Lampung,” Jurnal Teknologi dan Informatika (JEDA), vol. 5, no. 2, pp. 2745–8911, 2024.

[7] P. R. Calhoun, M. P. Montemurro, and D. Stanley, “Control and provisioning of wireless access points (CAPWAP) protocol specification,” RFC, vol. 5415, pp. 1–155, 2009, doi: 10.17487/RFC5415.

[8] Huawei Technologies Co., Ltd., Huawei Certification Training. Shenzhen, China: Huawei Technologies Co., Ltd., 2020. [Online]. Available: https://e.huawei.com/

[9] D. E. Ginanti, A. Christian, and T. Hidayat, "Analisa dan implementasi jaringan wireless MAC address menggunakan filtering pada PT. Faya Kuntura Agung Konsultindo," Inti Nusa Mandiri, vol. 16, no. 2, 2022, doi: 10.33480/inti.v16i2.2781.

[10] A. Fitriansyah, A. Andreansyah, and A. Sopian, "Penerapan static VLAN dan access list untuk meningkatkan keamanan jaringan," Jurnal Teknologi Informatika dan Komputer, vol. 5, no. 2, pp. 58–63, 2019, doi: 10.37012/jtik.v5i2.176.

[11] T. Lammle, CompTIA Network+ Study Guide. Hoboken, NJ, USA: Wiley, 2020.

[12] M. Tahir, Hariyanto, M. I. Firdausi, Saim, Nuriyah, and Maimunah, "Peningkatan keamanan jaringan LAN dan WLAN melalui standard access control list," Digital Transformation Technology, vol. 4, no. 1, pp. 607–614, 2024, doi: 10.47709/digitech.v4i1.4261.

[13] I. Widyastuti and Y. Hendrian, "Pemanfaatan VLAN untuk meningkatkan kinerja jaringan komputer BKPP Kabupaten Bogor," Computer Science (CO-SCIENCE), vol. 2, no. 1, pp. 10–18, 2022, doi: 10.31294/coscience.v2i1.894.

[14] M. Donni and L. Siahaan, "Implementation of wireless controller using Capsman (Controller Access Point System Manager) in computer laboratory of SMK Negeri 9 Medan," International Journal of Computer Sciences and Mathematics Engineering, vol. 2, no. 2, pp. 289–298, 2023, doi: 10.61306/ijecom.v2i2.55.

[15] S. Syafii, M. Tahir, M. Dani, N. Maulidya, and N. W. Haqiqi, "Perancangan sistem keamanan jaringan nirkabel dengan WPA2 Enterprise," Jurnal RESTIKOM, vol. 7, no. 1, pp. 74–86, 2025, doi: 10.52005/restikom.v71.415.