JURNAL ILMIAH FIFO
Vol. 18 No. 1 (2026) 22-30
DOI: 10.22441/fifo.2026.v18i1.003

P-ISSN 2085-4315
E-ISSN 2502-8332

Peningkatan Keamanan Jaringan melalui Penerapan VLAN dan ACL Berbasis NDLC

Reza Purnomo[1], Desi Ramayanti[2*]

[1,2]Universitas Dian Nusantara
Email: [1]411212070@mahasiswa.undira.ac.id, [2]desi.ramayanti@undira.ac.id
Penulis Korespondensi[*]

(***received*****:** 14-01-26, ***revised*****:** 19-01-26, ***accepted*****:** 23-01-26)

Abstrak

Infrastruktur jaringan komputer pada PT Bintang Barutama saat ini menghadapi kendala kinerja dan keamanan akibat penggunaan topologi flat network. Kondisi ini menyebabkan meluasnya broadcast domain yang memicu tingginya latensi jaringan hingga mencapai 1152 ms dan packet loss sebesar 30–32% di beberapa area operasional, serta meningkatkan risiko kebocoran data sensitif antar-divisi karena tidak adanya pembatasan akses. Penelitian ini bertujuan untuk merancang ulang arsitektur jaringan guna meningkatkan efisiensi lalu lintas data dan keamanan informasi perusahaan. Metode penelitian yang digunakan adalah Network Development Life Cycle (NDLC) yang mencakup tahap analisis, desain, dan simulasi menggunakan Cisco Packet Tracer. Solusi yang dirancang meliputi segmentasi jaringan menggunakan Virtual Local Area Network (VLAN), pengalamatan IP berbasis Variable Length Subnet Mask (VLSM), serta penerapan Extended Access Control List (ACL) untuk pengaturan hak akses antar-divisi. Berdasarkan hasil simulasi, penerapan VLAN dan ACL menunjukkan potensi penurunan latensi dan packet loss dibandingkan kondisi jaringan awal, seiring berkurangnya broadcast domain dan trafik antar-divisi yang tidak relevan. Temuan ini memberikan rencana teknis yang siap diimplementasikan pada lingkungan produksi dan dapat menjadi acuan bagi perusahaan dengan karakteristik jaringan serupa untuk melakukan transisi menuju sistem yang lebih aman dan efisien.

Kata Kunci: Network Development Life Cycle (NDLC), VLAN, Access Control List (ACL), Keamanan Jaringan, Cisco Packet Tracer.

Abstract

The computer network infrastructure at PT Bintang Barutama is currently experiencing performance and security problems due to the use of a flat network topology. This condition creates a large broadcast domain, which triggers high network latency of up to 1152 ms and packet loss of 30–32% in several operational areas, as well as increases the risk of sensitive data leakage between divisions because access restrictions are not applied. This study aims to redesign the network architecture to improve data traffic efficiency and information security. The research method used is the Network Development Life Cycle (NDLC), covering analysis, design, and simulation stages using Cisco Packet Tracer. The proposed solution includes network segmentation using Virtual Local Area Networks (VLAN), IP addressing using Variable Length Subnet Mask (VLSM), and the implementation of Extended Access Control Lists (ACL) to regulate access between divisions. Based on simulation results, the use of VLAN and ACL shows the potential to reduce latency and packet loss compared to the current condition, as the broadcast domain and non-relevant inter-division traffic are minimized. These findings provide a technical design ready for real implementation and can serve as a reference for companies with similar network characteristics transitioning toward a more secure and efficient system.

Keywords*: Network Development Life Cycle (NDLC), VLAN, Access Control List (ACL), Network Security, Cisco Packet Tracer.*

1. PENDAHULUAN

Dalam era globalisasi saat ini, infrastruktur teknologi informasi yang andal telah menjadi tulang punggung utama bagi keberlangsungan operasional sektor bisnis dan industri. Ketergantungan terhadap stabilitas jaringan menuntut organisasi untuk mengelola infrastruktur TI secara optimal guna menjamin keamanan dan kelancaran pertukaran data [1], [2]. Kualitas layanan jaringan atau Quality of Service (QoS) menjadi indikator vital; gangguan sekecil apa pun pada konektivitas dapat berdampak langsung pada produktivitas perusahaan [3]. Hal ini juga berlaku bagi PT Bintang Barutama, sebuah perusahaan distributor alat teknik di Jakarta Utara yang

P-ISSN 2085-4315
E-ISSN 2502-8332

sangat bergantung pada sistem informasi terpusat untuk mendukung divisi vital seperti warehouse, penjualan, IT, purchasing, HR, dan keuangan.

Namun, kondisi saat ini di PT Bintang Barutama menunjukkan adanya tantangan serius pada infrastruktur jaringan. Berdasarkan observasi awal, jaringan yang digunakan masih bersifat datar (*flat network*) tanpa segmentasi, sehingga menyebabkan *broadcast domain* menjadi sangat luas. Permasalahan ini diperparah oleh manajemen bandwidth yang belum optimal, sehingga memicu latensi yang tinggi hingga 1152 ms serta *packet loss* sebesar 30–32% di area operasional. Kondisi ini sejalan dengan temuan pada penelitian lain yang menyatakan bahwa pengaturan bandwidth yang buruk tanpa prioritas trafik dapat menurunkan kinerja jaringan secara signifikan [4]. Selain masalah kinerja, tidak adanya pembatasan akses menyebabkan lalu lintas non-produktif (seperti media sosial dan streaming) membebani jaringan serta membuka celah keamanan yang rentan terhadap ancaman siber.

Untuk mengatasi permasalahan kinerja dan keamanan tersebut, diperlukan restrukturisasi jaringan melalui penerapan teknologi segmentasi dan kontrol akses. Penelitian terdahulu menunjukkan bahwa penerapan Virtual Local Area Network (VLAN) efektif untuk memecah jaringan fisik menjadi segmen logis yang lebih kecil, sehingga membatasi penyebaran broadcast storm dan mempermudah manajemen jaringan [5]. Selain segmentasi, keamanan jaringan perlu diperkuat menggunakan Access Control List (ACL). Implementasi ACL terbukti mampu berfungsi sebagai filter lalu lintas data yang mengizinkan atau memblokir paket berdasarkan aturan keamanan yang ketat, sehingga dapat memitigasi akses ilegal antar-divisi [6], [7]. Integrasi antara VLAN dan ACL pada jaringan area luas maupun lokal telah terbukti meningkatkan efisiensi trafik sekaligus keamanan data instansi secara signifikan [8].

Berbagai penelitian sebelumnya telah membahas peningkatan kualitas dan keamanan jaringan melalui penerapan VLAN dan ACL. Studi oleh menunjukkan bahwa segmentasi VLAN mampu mengurangi trafik broadcast dan meningkatkan efisiensi jaringan pada instansi pendidikan [5]. Penelitian lain juga membuktikan bahwa ACL efektif membatasi akses pengguna dan mencegah kebocoran data pada jaringan multi-divisi [6]. Namun, sebagian besar penelitian tersebut hanya membahas implementasi VLAN atau ACL secara mandiri, atau tidak secara eksplisit mengevaluasi keduanya dalam satu kerangka metodologis yang terstruktur. Celah penelitian (research gap) ini menjadi dasar bagi penelitian ini untuk menggabungkan penerapan VLAN, VLSM, dan ACL dengan pendekatan NDLC serta memvalidasi hasilnya melalui simulasi. Dengan demikian, tujuan penelitian ini tidak hanya merancang ulang jaringan PT Bintang Barutama, tetapi juga memberikan pembuktian praktis bahwa kombinasi segmentasi dan kontrol akses dapat meningkatkan keamanan dan performa jaringan pada perusahaan distribusi dengan struktur multidivisi.

Berdasarkan latar belakang tersebut, penelitian ini berfokus pada analisis dan perancangan ulang keamanan jaringan di PT Bintang Barutama. Pendekatan yang digunakan adalah metode Network Development Life Cycle (NDLC) untuk memastikan tahapan pengembangan yang terstruktur mulai dari analisis hingga manajemen. Tujuan utama penelitian ini adalah merancang bangun arsitektur jaringan yang aman melalui segmentasi VLAN dan penerapan kebijakan ACL, serta mengukur efektivitasnya melalui simulasi menggunakan Cisco Packet Tracer sebelum diimplementasikan pada perangkat keras yang sesungguhnya.

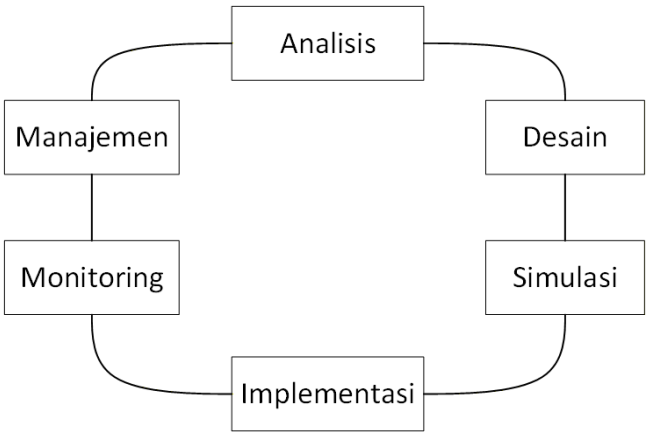
2. METODE PENELITIAN

Penelitian ini menerapkan pendekatan kualitatif deskriptif untuk memperoleh data yang akurat dan dapat dipertanggungjawabkan mengenai kondisi infrastruktur jaringan di PT Bintang Barutama. Proses pengumpulan data dilakukan melalui serangkaian tahapan sistematis, dimulai dengan observasi langsung ke lokasi untuk memetakan topologi fisik, jalur kabel, serta mengidentifikasi kendala teknis pada perangkat keras yang digunakan di lapangan. Tahapan ini mengacu pada kerangka analisis infrastruktur untuk memastikan validitas data fisik yang diperoleh [9]. Selanjutnya, dilakukan wawancara mendalam dengan staf IT dan kepala divisi terkait guna menggali informasi mengenai kebijakan manajemen jaringan, alur data antar-divisi, serta spesifikasi perangkat eksisting. Data primer tersebut kemudian didukung oleh studi pustaka yang bersumber dari jurnal ilmiah dan dokumentasi teknis terkait teknologi VLAN, Access Control List (ACL), serta simulasi jaringan menggunakan Cisco Packet Tracer [10].

Dalam merancang solusi jaringan, penelitian ini mengadopsi metode Network Development Life Cycle (NDLC) yang menyediakan kerangka kerja berkelanjutan untuk pengembangan infrastruktur. Menurut Rodianto, dkk., siklus NDLC terdiri dari enam tahapan utama, yaitu Analysis, Design, Simulation, Implementation, Monitoring, dan Management [11]. Namun, mengingat batasan ruang lingkup penelitian yang berfokus pada validasi desain arsitektur keamanan, proses pengembangan dalam studi ini dibatasi hingga tahap simulasi. Tahapan dimulai dengan Analysis untuk memetakan kebutuhan pengguna dan pola lalu lintas data, dilanjutkan dengan tahap Design untuk merancang topologi baru yang menerapkan segmentasi VLAN dan

JURNAL ILMIAH FIFO
Vol. 18 No. 1 (2026) 22-30
DOI: 10.22441/fifo.2026.v18i1.003
P-ISSN 2085-4315
E-ISSN 2502-8332

aturan ACL. Terakhir, dilakukan tahap Simulation menggunakan perangkat lunak untuk menguji konektivitas dan keamanan rancangan sebelum diterapkan secara nyata [12]. Struktur tahapan NDLC yang digunakan dalam penelitian ini ditunjukkan pada Gambar 1.



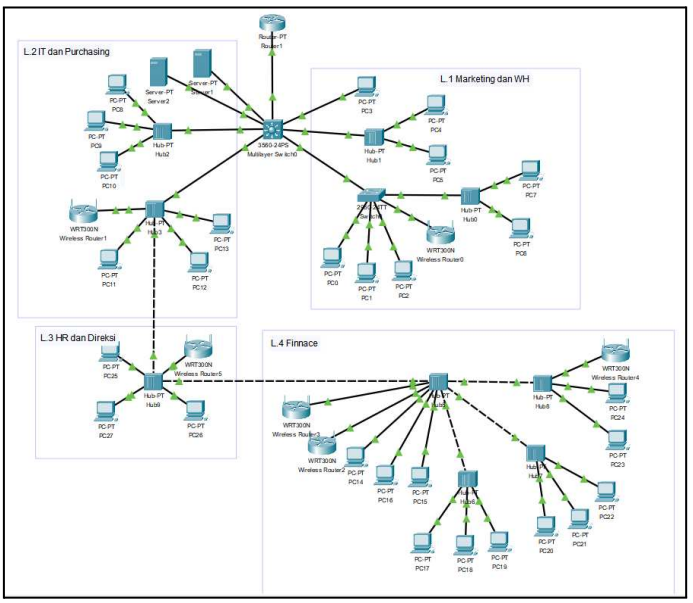
Gambar 1. Siklus Network Development Life Cycle (NDLC)

Penelitian ini menerapkan tiga tahap utama dalam siklus Network Development Life Cycle (NDLC), yaitu Analysis, Design, dan Simulation, sementara tahap Implementation, Monitoring, dan Management tidak dilakukan karena penelitian dibatasi pada simulasi jaringan. Pada tahap Analisis, data diperoleh melalui observasi langsung terhadap infrastruktur jaringan PT Bintang Barutama, wawancara dengan staf IT, penyebaran kuesioner kepada pengguna dari berbagai divisi, serta pengukuran awal Quality of Service (latency, packet loss, jitter, dan throughput). Proses ini menghasilkan gambaran menyeluruh kondisi jaringan eksisting, termasuk ditemukannya topologi flat network dengan broadcast domain tunggal, performa jaringan yang tidak stabil, dan ketiadaan kontrol akses antar-divisi. Hasil analisis selanjutnya menjadi dasar tahap Design, di mana dirancang topologi jaringan baru yang lebih terstruktur melalui pembagian Virtual Local Area Network (VLAN) berdasarkan divisi, pengalamatan IP berbasis Variable Length Subnet Mask (VLSM), penerapan Inter-VLAN Routing untuk kebutuhan komunikasi tertentu, serta penyusunan aturan Extended Access Control List (ACL) guna membatasi akses antar-divisi sesuai kebijakan keamanan. Desain ini juga mencakup penyesuaian skema DHCP agar alokasi IP dapat dilakukan secara otomatis dan terpisah per segmen jaringan. Tahap penutup adalah Simulation, di mana desain topologi tersebut diimplementasikan pada Cisco Packet Tracer melalui konfigurasi VLAN, routing, DHCP, dan ACL. Pengujian dilakukan untuk memastikan bahwa setiap segmen jaringan dapat berkomunikasi sesuai kebutuhan operasional dan bahwa ACL berhasil memblokir akses tidak sah antar-divisi. Selain itu, pengukuran ulang parameter QoS dibandingkan kondisi awal untuk memverifikasi adanya peningkatan performa dan efisiensi lalu lintas jaringan. Hasil simulasi inilah yang menjadi dasar penilaian efektivitas rancangan sebelum diimplementasikan pada lingkungan fisik.

Berdasarkan analisis terhadap sistem yang sedang berjalan, diketahui bahwa topologi jaringan PT Bintang Barutama saat ini menggunakan model Topologi Star di mana seluruh perangkat terhubung ke switch distribusi tanpa adanya segmentasi logis [13]. Distribusi jaringan diteruskan dari switch utama ke berbagai lantai menggunakan Hub atau Wireless Router tambahan, sehingga menciptakan arsitektur flat network. Kondisi ini menyebabkan seluruh departemen berada dalam satu Broadcast Domain yang sama, yang memicu tingginya lalu lintas broadcast, risiko tabrakan data (collision), serta beban kerja perangkat yang berlebihan. Dampak dari arsitektur ini adalah penurunan Quality of Service (QoS) yang signifikan, ditandai dengan koneksi yang lambat dan tidak stabil [3]. Oleh karena itu, perancangan ulang diperlukan untuk memecah domain jaringan tersebut guna meningkatkan efisiensi dan keamanan data. Gambaran kondisi topologi jaringan eksisting tersebut ditunjukkan pada Gambar 2.

JURNAL ILMIAH FIFO
Vol. 18 No. 1 (2026) 22-30
DOI: 10.22441/fifo.2026.v18i1.003

P-ISSN 2085-4315
E-ISSN 2502-8332



Gambar 2. Topologi Jaringan Saat Ini (Existing)

3. HASIL DAN PEMBAHASAN

3.1. Hasil Penelitian

A. Analisis Kebutuhan Sistem

Tahap awal penelitian dimulai dengan analisis mendalam terhadap infrastruktur existing di PT Bintang Barutama. Berdasarkan observasi, ditemukan bahwa topologi jaringan datar (flat network) yang digunakan saat ini memicu perluasan broadcast domain yang berlebihan, mengakibatkan penurunan kinerja jaringan. Analisis kebutuhan fungsional merekomendasikan segmentasi jaringan menjadi empat kelompok VLAN (Virtual Local Area Network) berdasarkan fungsi kerja dan tingkat sensitivitas data.

Rincian pembagian segmen tersebut dijabarkan dalam Tabel 1. Temuan menarik dari analisis ini adalah adanya kebutuhan lintas lokasi fisik, di mana terdapat tiga unit komputer yang secara fisik berada di ruang HR dan Finance, namun secara operasional membutuhkan akses data stok gudang. Oleh karena itu, perangkat tersebut dikonfigurasikan secara logis masuk ke dalam VLAN Operasional (VLAN 10) untuk menjamin integritas alur kerja distribusi barang tanpa terhalang batasan fisik ruangan.

Tabel 1. Kebutuhan Segmentasi VLAN dan Perangkat

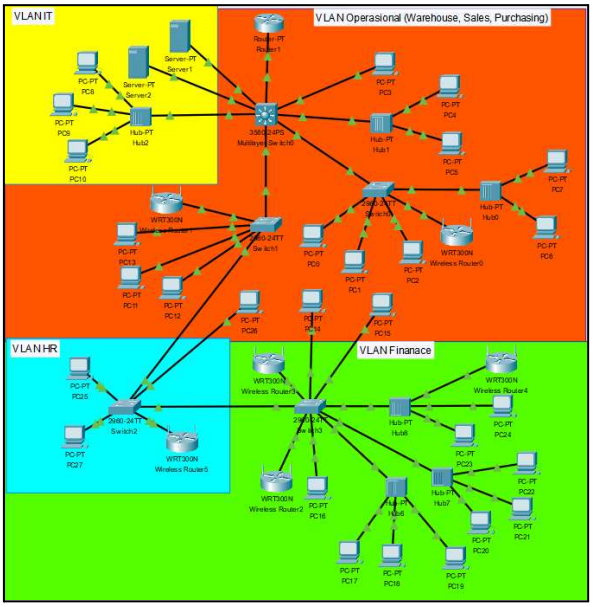
No	Nama Segmen	VLAN ID	Divisi/Unit Kerja	Kebijakan Akses
1	Operasional	10	Warehouse, Sales, Purchasing	Standar: Menggabungkan operasional lintas lokasi (Lantai 1 & 3).
2	IT Manager	20	Teknologi Informasi (IT)	Full Access: Akses penuh ke seluruh segmen untuk maintenance.
3	HR	30	Human Resources	Restricted: Isolasi jaringan untuk menjaga kerahasiaan data karyawan.
4	Finance	40	Finance & Accounting	High Security: Terisolasi total dari operasional untuk mencegah kebocoran data.

B. Perancangan Topologi dan Pengalamatan IP

Desain topologi usulan mengadopsi struktur hirarkis dengan Multilayer Switch (MLS) sebagai perangkat Core yang menangani Inter-VLAN Routing. Sebagaimana divisualisasikan pada Gambar 3, arsitektur jaringan

JURNAL ILMIAH FIFO
Vol. 18 No. 1 (2026) 22-30
DOI: 10.22441/fifo.2026.v18i1.003
P-ISSN 2085-4315
E-ISSN 2502-8332

dibagi menjadi empat zona logis yang terpisah secara visual: zona kuning (VLAN IT), zona oranye (VLAN Operasional), zona biru (VLAN HR), dan zona hijau (VLAN Finance). Seluruh Switch Distribution dan Access Point dari setiap zona terhubung secara terpusat (star topology) menuju MLS guna menjamin stabilitas lalu lintas data antar-divisi.



Gambar 3. Topologi Jaringan Usulan

Perangkat Hub lama diganti dengan Switch Managed untuk mendukung segmentasi ini. Skema pengalamatan IP dirancang menggunakan metode Variable Length Subnet Mask (VLSM). Penerapan VLSM ini sangat krusial untuk mengefisienkan alokasi host dan meminimalisir pemborosan alamat IP pada setiap subnet yang berbeda ukuran. Konfigurasi IP Address didistribusikan secara otomatis menggunakan DHCP Server yang terpusat di MLS. Rincian skema IP dan aturan dasar kebijakan akses dapat dilihat pada Tabel 2.

Tabel 2. Skema IP Address dan Kebijakan

VLAN ID	Nama Segmen	Subnet Network	Range Host (DHCP)	Deskripsi Kebijakan ACL
10	Operasional	192.168.10.0/24	.10 - .200	Restricted: Blokir akses ke VLAN 30 (HR) & 40 (Finance)
20	IT Manager	192.168.20.0/24	.10 - .200	Permit All: Akses penuh ke semua VLAN & Server.
30	HR	192.168.30.0/24	.50 - .200	Restricted: Hanya akses ke Server & Internet. Blokir ke Ops & Fin.
40	Finance	192.168.40.0/24	.50 - .200	High Security: Isolasi total dari VLAN lain.

C. Implementasi Konfigurasi

Implementasi teknis disimulasikan menggunakan Cisco Packet Tracer. Sesuai dengan tahapan simulasi dalam metode NDLC, konfigurasi difokuskan untuk memastikan validitas logika jaringan sebelum penerapan nyata [15]. Konfigurasi mencakup inisialisasi VLAN Database, penetapan mode trunking, serta pengaktifan Inter-VLAN Routing. Selain itu, aspek nirkabel (WLAN) juga dipertimbangkan pada segmen operasional untuk mendukung mobilitas perangkat, sebagaimana pendekatan NDLC yang efektif dalam perancangan jaringan kabel maupun nirkabel [16].

JURNAL ILMIAH FIFO
Vol. 18 No. 1 (2026) 22-30
DOI: 10.22441/fifo.2026.v18i1.003
P-ISSN 2085-4315
E-ISSN 2502-8332

Guna meningkatkan keamanan jaringan, diterapkan mekanisme Extended Access Control List (ACL). Kebijakan ini juga berfungsi sebagai mitigasi awal terhadap potensi serangan internal seperti DHCP Starvation atau akses ilegal, yang sering kali berdampak buruk terhadap performansi router jika tidak difilter dengan baik [17].

D. Pengujian Konektivitas (Verifikasi)

Pengujian dilakukan dalam dua fase: fase pertama memverifikasi Inter-VLAN Routing (konektivitas dasar), dan fase kedua memverifikasi keamanan (ACL). Rangkuman hasil akhir pengujian pada Tabel 3 memperlihatkan bahwa seluruh skenario telah valid.

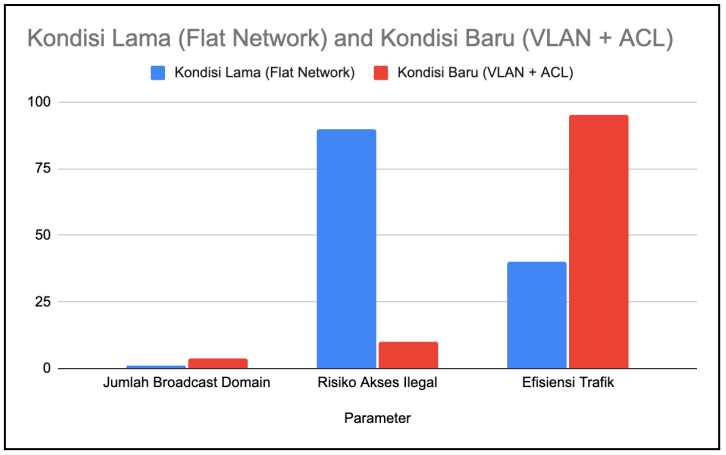
Tabel 3. Hasil Akhir Pengujian Konektivitas (Ping Test)

Source	Destination	Status	Kesimpuan
PC IT (Admin)	PC Operasional	Reply	Validasi (Ases admin berjalan)
PC Operasional	Server Kantor	Reply	Validasi (Ases admin berjalan)
PC Operasional	PC Finance	Dest. Unreacheable	Blokir Berhasil
PC HRD	PC Operasional	Dest. Unreacheable	Blokir Berhasil

3.2. Pembahasan

A. Analisis Efektivitas Segmentasi VLAN

Penerapan VLAN terbukti berhasil memecah broadcast domain tunggal menjadi empat segmen logis. Hal ini tidak hanya mengamankan data, tetapi juga mempermudah optimalisasi pengelolaan data antar-divisi. Seperti dalam studi kasus optimalisasi data akuntansi, pemisahan jalur akses yang jelas memungkinkan divisi Finance mengakses server basis data dengan lebih stabil tanpa gangguan trafik dari divisi lain [18]. Selain itu, segmentasi ini mempermudah proses monitoring infrastruktur jaringan kedepannya, karena trafik dapat dipantau per segmen (VLAN) untuk mendeteksi anomali dengan lebih cepat [19].



Gambar 4. Grafik kondisi sebelum dan sesudah VLAN+ACL

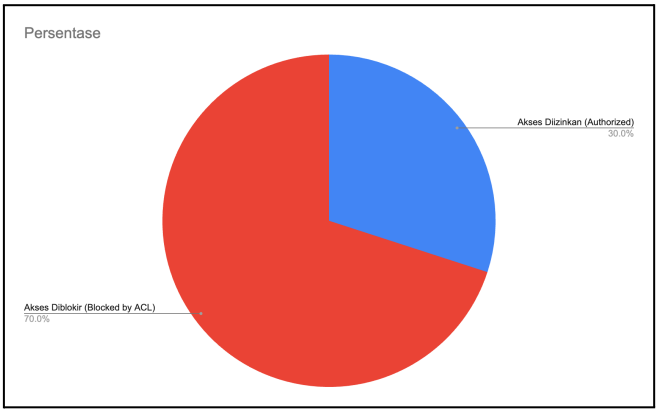
Visualisasi pada Gambar 4 menyajikan analisis komparatif dampak implementasi sistem. Pada kondisi awal (Flat Network), grafik menunjukkan tingkat risiko akses ilegal yang sangat tinggi (batang biru) disertai efisiensi trafik yang rendah, akibat tercampurnya seluruh lalu lintas data dalam satu broadcast domain.

Sebaliknya, pada kondisi baru (VLAN + ACL), terjadi perubahan parameter yang signifikan. Peningkatan jumlah broadcast domain (batang merah kecil) menandakan keberhasilan segmentasi dalam memecah jaringan. Hal ini berkorelasi positif dengan peningkatan efisiensi trafik dan penurunan risiko akses ilegal secara drastis, membuktikan bahwa isolasi jaringan efektif menutup celah keamanan dan mengoptimalkan penggunaan bandwidth. Hasil simulasi dalam penelitian ini juga menunjukkan arah peningkatan performa yang konsisten dengan studi sebelumnya mengenai penerapan VLAN dan ACL, walaupun pengukuran kuantitatif di jaringan fisik belum dilakukan.

JURNAL ILMIAH FIFO
Vol. 18 No. 1 (2026) 22-30
DOI: 10.22441/fifo.2026.v18i1.003
P-ISSN 2085-4315
E-ISSN 2502-8332

B. Analisis Keamanan dan Stabilitas

Pengujian ACL menunjukkan bahwa kebijakan keamanan mampu melindungi data sensitif. Isolasi trafik ini krusial untuk menjaga stabilitas jaringan. Meskipun penelitian ini belum menerapkan protokol redundansi penuh, desain VLAN yang terstruktur merupakan fondasi dasar untuk pengembangan sistem failover di masa depan guna menjamin keberlangsungan layanan [20].



Gambar 5. Persentase Dampak Penerapan ACL

Berdasarkan persentase kebijakan lalu lintas yang ditampilkan pada Gambar 5, terlihat bahwa arsitektur keamanan jaringan didominasi oleh aturan pemblokiran (Blocked by ACL) sebesar 70%. Angka dominan ini memvalidasi penerapan prinsip Least Privilege, di mana mayoritas jalur komunikasi antar-perangkat (seperti akses peer-to-peer lintas divisi) ditutup secara default untuk mencegah pergerakan lateral ancaman siber.

Sisa 30% lalu lintas yang berstatus Authorized merupakan jalur komunikasi esensial yang telah diverifikasi, meliputi akses pengguna ke server aplikasi, koneksi internet, serta jalur manajemen khusus bagi administrator IT. Proporsi ini menegaskan bahwa sistem keamanan bekerja secara ketat namun tetap mengakomodasi kebutuhan operasional utama.

C. Perbandingan Kinerja

Perubahan arsitektur dari flat network ke VLAN memberikan peningkatan signifikan pada Quality of Service (QoS). Pada kondisi awal, latensi tinggi sering terjadi akibat saturasi bandwidth. Dengan segmentasi, alokasi bandwidth menjadi lebih terjamin. Hal ini sejalan dengan temuan Ramayanti dan Syarifudin yang menyatakan bahwa analisis dan peningkatan kualitas layanan jaringan sangat bergantung pada manajemen trafik yang efisien untuk mendukung tugas operasional [21]. Selain itu, manajemen beban trafik melalui segmentasi ini bekerja selayaknya prinsip load balancing dasar, di mana beban jaringan didistribusikan secara proporsional ke masing-masing VLAN untuk mencegah penumpukan data pada satu titik [22].

4. KESIMPULAN

Berdasarkan seluruh tahapan penelitian yang telah dilaksanakan menggunakan metode Network Development Life Cycle (NDLC), dapat disimpulkan bahwa perancangan ulang infrastruktur jaringan di PT Bintang Barutama telah berhasil menjawab permasalahan latensi dan keamanan data yang sebelumnya terjadi. Transformasi arsitektur dari model flat network menjadi jaringan tersegmentasi berbasis Virtual Local Area Network (VLAN) terbukti efektif memecah broadcast domain tunggal menjadi empat segmen logis terpisah, yaitu Operasional, IT Manager, HR, dan Finance. Pemisahan ini secara signifikan mengeliminasi lalu lintas broadcast yang tidak relevan antar-divisi sehingga alokasi bandwidth menjadi lebih efisien. Selanjutnya, penerapan keamanan menggunakan Extended Access Control List (ACL) dengan prinsip Least Privilege telah terverifikasi valid melalui pengujian simulasi. Mekanisme ini mampu memblokir 100% akses ilegal antar-divisi demi menjaga kerahasiaan data sensitif, namun tetap menjamin ketersediaan akses (Availability) menuju server dan internet bagi pengguna yang berhak. Selain itu, penggunaan skema pengalamatan VLSM dan konfigurasi VLAN terbukti memberikan fleksibilitas tinggi dalam mengatasi kendala batasan fisik gedung, di mana

P-ISSN 2085-4315
E-ISSN 2502-8332

perangkat yang tersebar di lokasi berbeda tetap dapat dikelola dalam satu manajemen jaringan logis yang terpusat dan aman.

DAFTAR PUSTAKA

[1] D. Ramayanti and V. Saputra, "Optimasi Infrastruktur Wi-Fi dan Manajemen Bandwidth di Sekolah Menengah Pertama Menggunakan Teknologi Mikrotik," Arcitech: Journal of Computer Science and Artificial Intelligence, vol. 5, no. 1, pp. 1–17, Jun. 2025.

[2] G. M. Taberima and D. Ramayanti, "Mengoptimalkan Manajemen dan Keamanan TI Melalui Implementasi Layanan Domain Active Directory Studi Kasus pada Infrastruktur TI Perusahaan," Jinteks (Jurnal Informatika Teknologi dan Sains), vol. 6, no. 1, pp. 79-89, 2024.

[3] T. Zibaltar and D. Ramayanti, "Analisis Kualitas Jaringan Internet di Gedung Guntur: Studi Kasus pada Tenant Call Center PT Jasnita Telekomindo," JSAI (Journal Sci. Appl. Informatics), vol. 6, no. 3, pp. 280-290, 2024.

[4] N. Asyifah and D. Ramayanti, "Optimasi Kinerja Jaringan Di SMK Al Fudhola Bekasi: Pengaturan Bandwidth Dengan Mikrotik RB 951ui-2hnd Dan Penerapan Algoritma Simple Queue," J. Ilm. Ilk. - Ilmu Komput. Inform., vol. 7, no. 1, pp. 33–46, Jan. 2024.

[5] K. I. Ramadhan and A. Junaidi, "Perancangan Jaringan VLAN Sekolah Menengah Atas Fatahillah," CONTEN (Computer Networking Technology), vol. 4, no. 1, pp. 58–65, Jun. 2024.

[6] F. Fahrizal and B. A. Candra, "Implementasi Access Control List dalam Perancangan Virtual Local Area Network pada PT Cakramedia Indocyber," JEIS (Jurnal Elektro dan Informatika Swadharma), vol. 2, no. 2, pp. 36–43, Jul. 2022.

[7] A. Al-furqan Abra and A. Syarif Aziz, "Implementasi Access Control List (ACL) dalam Perancangan Virtual Local Area Network pada SMKN 1 Al-Mubarkeya," JATI (Jurnal Mahasiswa Teknik Informatika), vol. 9, no. 1, pp. 368–373, Dec. 2024.

[8] D. P. Agustio and E. R. Nainggolan, "Penerapan Virtual Local Area Network Pada Jaringan MAN dengan Metode Filtering Berbasis Access Control List di Dinas Komunikasi dan Informatika Kota Serang," Jurnal Sistem Informasi, vol. 1, 2023.

[9] A. K. Septuvania and G. Purnama, "Analisis dan Perancangan Jaringan Infrastruktur Sekolah MTS Al-Ihsan," J. Inform. Dan Tek. Elektro Terap., vol. 11, no. 3, Aug. 2023.

[10] R. P. Wijoyo and S. D. Asri, "Perancangan Infrastruktur Jaringan di Kantor dengan Simulasi Menggunakan Packet Tracer (Studi Kasus di V2 Service Center)," Jurnal Teknologi, vol. 8, no. 4, 2024.

[11] R. Rodianto, I. Idham, Y. Yuliadi, M. T. A. Zaen, and W. Ramadhan, "Penerapan Network Development Life Cycle (NDLC) dalam Pengembangan Jaringan Komputer pada Badan Pengelolaan Keuangan dan Aset Daerah (BPKAD) Provinsi NTB," Jurnal Matrik, vol. 14, no. 1, 2022.

[12] H. Harjanto and G. Purnama, "Perancangan dan Simulasi Jaringan Komputer dengan Metode Pengembangan Network Development Life Cycle (NDLC) pada Kantor Cabang PT. V2 Indonesia," JATI (Jurnal Mahasiswa Teknik Informatika), vol. 8, no. 4, pp. 8032–8039, Aug. 2024.

[13] A. Nurarifin, R. Hidayathika, F. Fiana, R. Desfiana, and D. Aribowo, "Pengujian Kinerja Jaringan Topologi STAR dengan Switching: Studi Simulasi Menggunakan Cisco Packet Tracer," Jupiter: Publikasi Ilmu Keteknikan Industri, Teknik Elektro dan Informatika, vol. 2, no. 3, pp. 145–150, May 2024.

[14] T. Tamrin, N. Muhaidi, A. F. Arifin, and Ariyanto, "Implementasi Metode VLSM (Variable Length Subnet Mask) pada Pemetaan IP Address LAN (Local Area Network) di Lab Fakultas Saint dan Teknologi (FST) Unisnu Jepara," *J. Publ. Tek. Inform.*, vol. 2, no. 1, pp. 6–11, Jan. 2023.

[15] A. N. Hasan and G. Purnama, "Perancangan dan Simulasi Jaringan Internet Dengan Menerapkan Metode Pengembangan NDLC (Network Development Life Cycle) Pada Akses Education Centre," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 8, no. 3, pp. 2575-2585, 2024.

[16] D. Saputra and B. Y. Geni, "Analisa dan Perancangan Jaringan Wireless Local Area Network (WLAN) dengan Menggunakan Metode NDLC (Studi Kasus: Di Toko Besi Kunciran Baja)," *Jurnal Mahasiswa*, vol. 8, no. 2, 2024.

[17] D. Novianto, Y. S. Japriadi, L. Tommy, and Sujono, "Mitigasi DHCP Starvation Attack pada Routerboard Mikrotik dan Pengaruhnya Terhadap Performansi," *J. Ilm. Inform. Glob.*, vol. 15, no. 2, pp. 52–57, Jul. 2024.

P-ISSN 2085-4315
E-ISSN 2502-8332

[18] Y. Andrian and D. Ramayanti, "Optimalisasi Pengolahan Data Akuntansi Accurate dengan Penerapan Server Database dan VPN menggunakan Metode Point-to-Point Tunneling Protocol (PPTP) di PT Indosterling Group," *PETIR (Jurnal Pengkajian Dan Penerapan Teknik Informatika)*, vol. 16, no. 2, pp. 173-188, 2023.

[19] K. Rivaldi and G. Purnama, "Perancangan dan Penerapan Monitoring Infrastruktur Perangkat Jaringan Komputer pada Pusat Data dan Sarana Informatika melalui Pengaplikasian Zabbix Network Engineering," *Jurnal Adijaya Multidisplin*, vol. 3, no. 04, pp. 589-611, 2023.

[20] V. R. Dewi and G. Purnama, "Perancangan Jaringan Sistem Failover Dengan Metode Hot Standby Routing Protocol (HSRP) Studi Kasus Di Yayasan Sukses Abadi," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 8, no. 1, pp. 339-345, 2024.

[21] D. Ramayanti and S. Syarifudin, "Analisis dan Peningkatan Kualitas Layanan Pada Jaringan Komputer Nirkabel Badan Penghubung Lampung Dalam Mendukung Tugas Pemerintahan," *JSAI (Journal Scientific and Applied Informatics)*, vol. 7, no. 1, pp. 1-13, 2024.

[22] A. Mustofa and D. Ramayanti, "Implementasi Load Balancing dan Failover to Device Mikrotik Router Menggunakan Metode NTH (Studi Kasus: PT. GO-JEK Indonesia)," *Jurnal Teknologi Informasi Dan Ilmu Komputer*, vol. 7, no. 1, p. 139, 2020.