Jurnal Teknik Informatika dan Teknologi Informasi
Volume 6, Nomor 2, Agustus 2026
e-ISSN: 2827-9387, p-ISSN: 2827-9379, Hal. 517-528
DOI: https://doi.org/10.55606/jutiti.v6i2.7682
Tersedia: https://journalshub.org/index.php/jutiti

Perancangan Jaringan untuk Pengembangan Infrastruktur Kantor menggunakan Metode NDLC

Febriansyah
Program Studi Teknik Informatika, Universitas Dian Nusantara, Indonesia
**Penulis Korespondensi: 411221028@mahasiswa.undira.ac.id*

Abstract. *The development of a company's operational needs requires a more structured, efficient, and adaptive computer network infrastructure that can support organizational growth. The expansion of the office from one shophouse unit into two shophouse units increases the need for wireline and wireless networks capable of supporting user connectivity, work devices, internet access, and supporting devices such as CCTV. This research aims to design a wireline and wireless network that supports the development of office infrastructure using the Network Development Life Cycle (NDLC) method. The proposed design includes network topology planning, structured IP addressing, network segmentation using Virtual Local Area Network (VLAN), guest network access restriction, and multi-ISP connectivity through failover and failback mechanisms. The network simulation was carried out using GNS3 with MikroTik CHR as the main device to perform routing, VLAN, DHCP, NAT, firewall, and failover functions. The test results show that each client can obtain an IP address according to its respective VLAN, connect to the gateway, and access the internet. VLAN segmentation successfully separates the network based on its functions, namely Admin, Operational, CCTV, and Guest WiFi. Firewall testing shows that the Guest network can still access the internet but cannot access the internal network. In addition, the failover and failback mechanisms successfully operate when the primary ISP link is disabled and re-enabled. Thus, the proposed network design is able to represent the needs of office infrastructure development in a more structured manner and in accordance with the research objectives.*

Keywords: *Failover; GNS3; Multi-ISP; NDLC; VLAN; Wireless; Wireline*

Abstrak. Perkembangan kebutuhan operasional perusahaan mendorong perlunya pengembangan infrastruktur jaringan komputer yang lebih terstruktur, efisien, dan mampu menyesuaikan dengan pertumbuhan organisasi. Pengembangan kantor dari satu ruko menjadi dua ruko meningkatkan kebutuhan terhadap jaringan *wireline* dan *wireless* yang dapat mendukung konektivitas pengguna, perangkat kerja, akses internet, dan perangkat pendukung seperti CCTV. Penelitian ini bertujuan untuk merancang jaringan *wireline* dan *wireless* yang mampu mendukung pengembangan infrastruktur kantor dengan menggunakan metode *Network Development Life Cycle* (NDLC). Rancangan yang dibuat meliputi penyusunan topologi jaringan, skema pengalamatan IP yang terstruktur, segmentasi jaringan menggunakan *Virtual Local Area Network* (VLAN), pembatasan akses jaringan tamu, serta konektivitas *multi-ISP* melalui mekanisme *failover* dan *failback*. Simulasi jaringan dilakukan menggunakan GNS3 dengan *MikroTik CHR* sebagai perangkat utama untuk menjalankan fungsi *routing*, VLAN, DHCP, NAT, *firewall*, dan *failover*. Hasil pengujian menunjukkan bahwa setiap *client* dapat memperoleh IP Address sesuai dengan VLAN masing-masing, terhubung ke *gateway*, dan mengakses internet. Segmentasi VLAN berhasil memisahkan jaringan berdasarkan fungsi, yaitu Admin, Operasional, CCTV, dan Guest WiFi. Pengujian *firewall* menunjukkan bahwa jaringan Guest tetap dapat mengakses internet, namun tidak dapat mengakses jaringan internal. Selain itu, mekanisme *failover* dan *failback* berhasil berjalan ketika jalur ISP utama dinonaktifkan dan diaktifkan kembali. Rancangan jaringan yang dibuat mampu merepresentasikan kebutuhan pengembangan infrastruktur kantor secara lebih terstruktur dan sesuai dengan tujuan penelitian.

Kata Kunci: *Failover; GNS3; Multi-ISP; NDLC; VLAN; Wireless; Wireline*

1. LATAR BELAKANG

Perkembangan dunia usaha yang semakin kompetitif menuntut perusahaan untuk memperkuat infrastruktur kerjanya agar operasional tetap berjalan efektif. Salah satu bentuk penguatan tersebut adalah pengembangan infrastruktur kantor, misalnya dari satu lokasi menjadi dua area kerja. Perubahan ini secara langsung meningkatkan kebutuhan terhadap sistem teknologi informasi yang lebih baik, terutama jaringan komputer sebagai tulang punggung aktivitas operasional (Tanenbaum & Wetherall, 2011).

Naskah Masuk: 03 Mei 2026; Revisi: 10 Juni 2026; Diterima: 21 Juli 2026; Tersedia: 31 Juli 2026

Jaringan komputer modern tidak hanya berfungsi sebagai media komunikasi antarperangkat, tetapi juga sebagai penghubung aplikasi bisnis, basis data, dan layanan internet. Ketika perusahaan bertambah besar, jaringan yang awalnya dirancang sederhana sering kali perlu dikembangkan agar mampu menyesuaikan dengan kebutuhan operasional yang semakin kompleks. Hal ini terlihat dari kebutuhan konektivitas yang meningkat, pengalamatan IP yang belum terstruktur, ketiadaan segmentasi jaringan, hingga belum adanya mekanisme redundansi koneksi internet yang terdokumentasi dengan baik (Ajiji et al., 2021). Kondisi tersebut dapat memengaruhi produktivitas karena berdampak pada pengelolaan jaringan, komunikasi internal, dan risiko keamanan informasi (Abdelhalim et al., 2020).

Untuk mengatasi tantangan tersebut, diperlukan perancangan jaringan yang lebih komprehensif. Integrasi *wireline* dan *wireless* menjadi penting karena keduanya memiliki keunggulan yang berbeda, yaitu *wireline* menawarkan kestabilan dan keamanan, sedangkan *wireless* memberikan fleksibilitas dan mendukung mobilitas karyawan (Nourildean & Mohammed, 2023). Selain itu, penerapan VLAN memberikan pemisahan lalu lintas data agar lebih aman dan efisien sekaligus mempermudah manajemen perangkat dan *troubleshooting* (Abdelhalim et al., 2020). Penggunaan *multi-ISP* dengan mekanisme *failover* dan *failback* juga diperlukan sebagai bentuk redundansi koneksi internet agar akses tetap tersedia ketika jalur utama mengalami gangguan dan dapat kembali menggunakan jalur utama setelah koneksi normal (Amalia et al., 2023). Konsep serupa juga terbukti efektif untuk menjaga kontinuitas layanan pada jaringan perusahaan (Prasetyo, 2022).

Untuk merancang solusi jaringan secara sistematis, penelitian ini menggunakan metode *Network Development Life Cycle* (NDLC). Metode ini memberikan tahapan yang runtut mulai dari identifikasi kebutuhan, perencanaan, analisis, perancangan, simulasi, pengujian, hingga evaluasi (Sofana, 2016). Dengan pendekatan tersebut, rancangan jaringan tidak hanya menjawab kebutuhan saat ini, tetapi juga siap menyesuaikan dengan perkembangan perusahaan di masa mendatang karena jaringan harus mampu mengikuti dinamika operasional yang terus berubah.

Beberapa penelitian terdahulu memberikan kontribusi penting dalam mendukung pengembangan jaringan komputer yang lebih efisien, aman, dan andal. Penerapan VLAN terbukti mampu meningkatkan performa jaringan dengan mengurangi *broadcast domain*, meningkatkan efisiensi penggunaan *bandwidth*, dan memperkuat keamanan melalui pemisahan lalu lintas data (Ajiji et al., 2021). Pada konteks jaringan *wireless*, integrasi VLAN juga membantu pengelolaan trafik secara lebih terstruktur sehingga mendukung mobilitas kerja karyawan (Nourildean & Mohammed, 2023). Di sisi ketersediaan internet, pemanfaatan lebih

dari satu ISP dapat menjaga konektivitas ketika salah satu jalur mengalami gangguan (Amalia et al., 2023).

Berdasarkan kajian tersebut, peningkatan kualitas jaringan tidak hanya bergantung pada perangkat yang digunakan, tetapi juga pada perancangan arsitektur jaringan yang tepat, meliputi segmentasi VLAN, pengelolaan jaringan *wireless*, pengalamatan IP yang terstruktur, serta pemanfaatan *multi-ISP*. Melalui penelitian ini, penulis bertujuan menghasilkan rancangan jaringan *wireline* dan *wireless* yang lebih terstruktur untuk mendukung pengembangan infrastruktur kantor dari satu ruko menjadi dua ruko. Rancangan difokuskan pada penyusunan topologi, segmentasi VLAN, skema pengalamatan IP, pembatasan akses jaringan tamu, serta konektivitas *multi-ISP* berbasis *failover* dan *failback*, sehingga jaringan menjadi lebih stabil, aman, mudah dikelola, dan siap dikembangkan sesuai kebutuhan operasional perusahaan di masa mendatang (Sofana, 2016).

2. KAJIAN TEORITIS

Grand theory yang mendasari penelitian ini adalah *Network Development Life Cycle* (NDLC), yaitu pendekatan sistematis dalam merancang dan mengembangkan jaringan komputer melalui tahapan yang runtut, mulai dari identifikasi kebutuhan, perencanaan, analisis, perancangan, simulasi, pengujian, hingga evaluasi (Sofana, 2016). NDLC dipandang penting karena tanpa kerangka kerja yang jelas, perancangan jaringan berisiko tidak sesuai kebutuhan dan sulit dikelola. Penerapan NDLC dalam pengembangan infrastruktur jaringan komputer terbukti mampu menghasilkan rancangan yang lebih terarah dan sesuai kebutuhan organisasi (Prasetyo et al., 2025). Metode ini juga telah digunakan sebagai kerangka kerja utama pada perancangan infrastruktur LAN dengan model hierarkis (Hayati & Kurniawan, 2016). Pada lingkungan pendidikan maupun perkantoran, kombinasi NDLC dengan segmentasi VLAN menghasilkan jaringan yang lebih rapi dan mudah dikembangkan (Setiawan et al., 2024).

Teori pendukung utama dalam penelitian ini mencakup segmentasi jaringan menggunakan *Virtual Local Area Network* (VLAN), integrasi *wireline* dan *wireless*, serta ketersediaan koneksi internet melalui *multi-ISP*. Penerapan VLAN mampu meningkatkan performa jaringan dengan mengurangi *broadcast domain* sekaligus memperkuat keamanan melalui pemisahan lalu lintas antar divisi (Ajiji et al., 2021). Konsep tersebut diperkuat dengan mekanisme *inter-VLAN routing* yang menjaga komunikasi antar segmen tetap terkontrol pada jaringan korporat (Abdelhalim et al., 2020). Pada jaringan nirkabel, penerapan VLAN dapat menurunkan delay dan *packet loss* sehingga pengelolaan trafik menjadi lebih terstruktur

(Nourildean & Mohammed, 2023). Sementara itu, ketersediaan internet dijaga melalui pemanfaatan lebih dari satu ISP dengan teknik *load balancing* dan *failover* berbasis *Per Connection Classifier* pada *router* MikroTik (Amalia et al., 2023). Studi lain menegaskan bahwa penggunaan dua ISP dengan mekanisme *load balancing* dan *failover* mampu meningkatkan kinerja serta kontinuitas layanan jaringan (Azmi et al., 2022).

3. METODE PENELITIAN

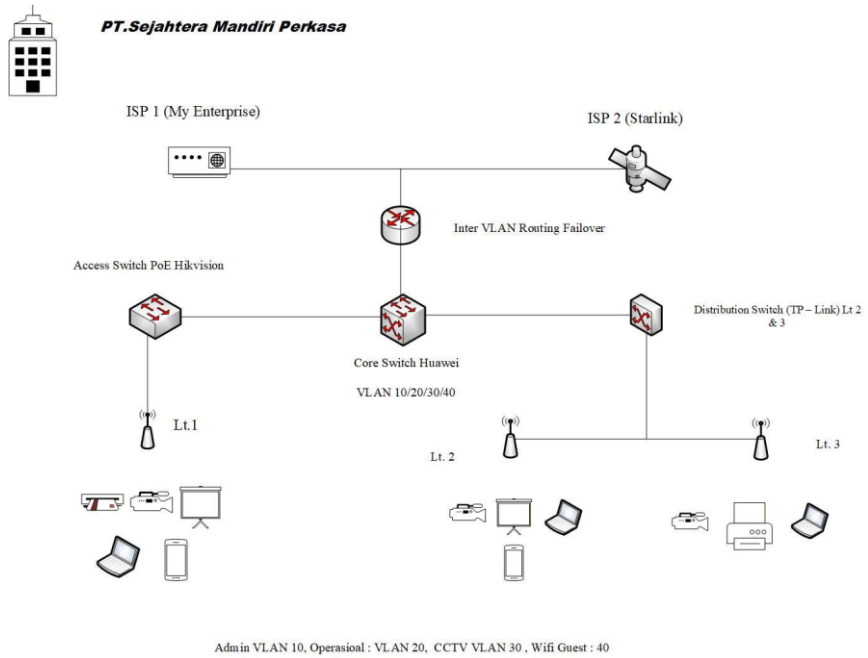
Penelitian ini merupakan penelitian terapan (*applied research*) yang berorientasi pada solusi praktis berupa rancangan jaringan komputer yang dapat diimplementasikan pada perusahaan. Subjek penelitian adalah infrastruktur jaringan PT Sejahtera Mandiri Perkasa pada Head Office Project Palm, Jakarta Barat, yang sedang berkembang dari satu ruko menjadi dua ruko sehingga memerlukan jaringan yang lebih andal, efisien, dan adaptif. Perancangan disusun menggunakan metode *Network Development Life Cycle* (NDLC) sebagai kerangka kerja (Sofana, 2016). Instrumen pengumpulan data yang digunakan meliputi observasi langsung terhadap kondisi fisik jaringan, penempatan perangkat, dan alur koneksi; wawancara terstruktur dengan pihak IT Presales Supervisor mengenai kebutuhan operasional, stabilitas internet, dan kendala teknis; serta studi dokumentasi terhadap topologi eksisting, daftar perangkat jaringan, dan alokasi IP Address. Rancangan jaringan diuji menggunakan perangkat lunak simulasi GNS3 dengan *MikroTik CHR* sebagai perangkat utama untuk menjalankan fungsi *routing*, VLAN, DHCP, NAT, *firewall*, serta *failover*.

Prosedur penelitian dilaksanakan secara kronologis mengikuti tahapan NDLC. Tahap awal berupa identifikasi masalah terhadap jaringan eksisting, dilanjutkan studi literatur, serta observasi dan wawancara untuk memperoleh data lapangan. Data tersebut dianalisis untuk menentukan kebutuhan jaringan, yang kemudian diterjemahkan pada tahap perancangan berupa penyusunan topologi, segmentasi VLAN, skema pengalamatan IP, konfigurasi *gateway*, koneksi *multi-ISP*, serta pembatasan akses jaringan tamu. Rancangan tersebut disimulasikan dan dikonfigurasikan pada lingkungan GNS3, lalu diuji dan dievaluasi. Analisis data dilakukan secara deskriptif melalui pengujian fungsional dengan pendekatan *black box*, yaitu membandingkan keluaran pengujian terhadap kriteria keberhasilan yang telah ditentukan. Indikator keberhasilan meliputi keberhasilan *client* memperoleh IP Address sesuai VLAN, konektivitas ke *gateway* dan internet, pembatasan akses jaringan Guest terhadap jaringan internal, serta berjalannya mekanisme *failover* dan *failback* ketika jalur ISP utama dinonaktifkan dan diaktifkan kembali.

4. HASIL DAN PEMBAHASAN

Topologi dan Rancangan Jaringan Usulan

Berdasarkan hasil tahap analysis pada metode NDLC, jaringan eksisting belum memiliki segmentasi yang jelas, masih bergantung pada satu ISP, dan belum terdokumentasi dengan baik. Oleh karena itu, disusun rancangan jaringan usulan yang lebih terstruktur menggunakan pendekatan topologi hierarkis (core, distribution, dan access). Jaringan usulan memanfaatkan dua koneksi internet, yaitu ISP1-MyEnterprise sebagai jalur utama dan ISP2-Starlink sebagai jalur cadangan, yang keduanya terhubung ke R-Mikrotik-*Gateway*. *Router* tersebut berperan sebagai pusat pengaturan trafik yang menangani *routing*, *inter-VLAN routing*, DHCP, NAT, *firewall*, serta mekanisme *failover*. Dari *router*, koneksi diteruskan ke SW-Core-Huawei sebagai pusat distribusi VLAN, kemudian ke SW-POE-Hikvision pada lantai 1 serta SW-Distribusi-TPLink untuk lantai 2 dan lantai 3 melalui jalur *trunk* VLAN.



Gambar 1. Diagram Topologi Jaringan Usulan.

Gambar 1 memperlihatkan bahwa jaringan dibagi menjadi empat segmen VLAN sesuai fungsinya, yaitu VLAN 10 untuk Admin, VLAN 20 untuk Operasional, VLAN 30 untuk CCTV, dan VLAN 40 untuk Guest WiFi. Pembagian tersebut bertujuan agar trafik antar kelompok pengguna dan perangkat dapat dipisahkan secara logis, sehingga keamanan dan pengelolaan jaringan menjadi lebih baik. Perangkat CCTV pada lantai 2 dan lantai 3 tetap ditempatkan pada VLAN 30 meskipun melewati *switch* distribusi, sehingga trafik pengawasan tidak bercampur dengan trafik pengguna internal maupun jaringan tamu. Rincian segmentasi VLAN beserta skema pengalamatan IP Address yang terstruktur ditunjukkan pada Tabel 1.

Tabel 1. Segmentasi VLAN dan Skema Pengalamatan IP Address.

VLAN	Fungsi / Segmen	Network	*Gateway*
VLAN 10	Admin	192.168.10.0/24	192.168.10.1
VLAN 20	Operasional	192.168.20.0/24	192.168.20.1
VLAN 30	CCTV	192.168.30.0/24	192.168.30.1
VLAN 40	Guest WiFi	192.168.40.0/24	192.168.40.1

Tabel 1 menunjukkan bahwa setiap VLAN memiliki network dan *gateway* yang terpisah. VLAN 10 Admin menggunakan network 192.168.10.0/24 dengan *gateway* 192.168.10.1, VLAN 20 Operasional menggunakan 192.168.20.0/24 dengan *gateway* 192.168.20.1, VLAN 30 CCTV menggunakan 192.168.30.0/24 dengan *gateway* 192.168.30.1, dan VLAN 40 Guest WiFi menggunakan 192.168.40.0/24 dengan *gateway* 192.168.40.1. Seluruh *gateway* tersebut berada pada *interface* VLAN di R-Mikrotik-*Gateway*. Skema pengalamatan yang terstruktur ini mempermudah pengelolaan perangkat, mengurangi potensi konflik alamat, dan mendukung administrasi jaringan yang lebih efisien. Peran masing-masing perangkat pada rancangan usulan diringkas pada Tabel 2.

Tabel 2. Perangkat Jaringan dan Perannya pada Rancangan Usulan.

Perangkat	Peran dalam Jaringan
R-Mikrotik-*Gateway*	*Router* utama: *routing*, *inter-VLAN routing*, DHCP server, NAT, *firewall*, dan *failover*
SW-Core-Huawei	Core *switch*: pusat distribusi VLAN melalui jalur *trunk*
SW-Distribusi-TPLink	*Switch* distribusi/access Layer 2 untuk lantai 2 dan lantai 3
SW-POE-Hikvision	Access *switch* PoE lantai 1 untuk CCTV dan *access point*
ISP1-MyEnterprise	Koneksi internet utama (*gateway* 10.10.10.1, distance 1)
ISP2-Starlink	Koneksi internet cadangan (*gateway* 20.20.20.1, distance 2)

Tabel 2 memperlihatkan pembagian fungsi perangkat yang jelas antara *router* dan *switch*. Seluruh fungsi Layer 3, seperti *routing*, *inter-VLAN routing*, DHCP, NAT, *firewall*, dan *failover*, dijalankan oleh R-Mikrotik-*Gateway*, sedangkan SW-Distribusi-TPLink hanya berperan sebagai *switch* Layer 2 yang meneruskan trafik VLAN. SW-Core-Huawei berfungsi sebagai pusat distribusi VLAN melalui *trunk*, dan SW-POE-Hikvision menyediakan koneksi data sekaligus daya bagi perangkat CCTV dan *access point* pada lantai 1. Pembagian peran ini menjaga alur jaringan tetap terstruktur dan memudahkan proses *troubleshooting* maupun pengembangan di masa mendatang.

Skenario dan Kriteria Pengujian

Pengujian dilakukan menggunakan metode *black box* yang berfokus pada verifikasi fungsi utama jaringan tanpa memeriksa detail konfigurasi internal. Pengujian mencakup segmentasi VLAN, konektivitas *gateway* pada setiap VLAN, pemberian IP Address melalui DHCP, akses internet melalui NAT, pembatasan akses jaringan Guest, serta mekanisme *failover* dan *failback*. Kriteria keberhasilan setiap pengujian ditunjukkan pada Tabel 3.

Tabel 3. Skenario dan Kriteria Keberhasilan Pengujian.

Pengujian	Kriteria Keberhasilan
Konektivitas *gateway* VLAN	*Client* pada setiap VLAN dapat melakukan ping ke *gateway* VLAN masing-masing
Segmentasi VLAN	Setiap *endpoint* berada pada jaringan IP dan VLAN yang sesuai dengan fungsi perangkatnya
Trunk antar perangkat	VLAN 10, 20, 30, dan 40 dapat melewati jalur *trunk* menuju *router gateway*
Akses internet melalui NAT	*Client* jaringan internal dapat mengakses alamat internet simulasi melalui *router gateway*
Firewall jaringan Guest	*Client* Guest tidak dapat mengakses jaringan Admin, Operasional, dan CCTV, tetapi tetap dapat mengakses internet
Failover koneksi internet	Ketika ISP utama tidak aktif, koneksi internet berpindah ke ISP cadangan
Failback koneksi internet	Ketika ISP utama aktif kembali, koneksi internet kembali menggunakan jalur ISP utama

Tabel 3 menjadi acuan objektif dalam menilai keberhasilan rancangan. Pengujian dinyatakan berhasil apabila setiap *client* dapat terhubung ke *gateway* VLAN masing-masing, jalur *trunk* mampu membawa seluruh VLAN menuju *router*, jaringan internal dapat mengakses internet melalui NAT, *firewall* dapat membatasi akses jaringan Guest terhadap jaringan internal, serta mekanisme *failover* dan *failback* berjalan sesuai skenario. Apabila hasil pengujian belum memenuhi kriteria, dilakukan evaluasi dan perbaikan terhadap konfigurasi VLAN, DHCP, *routing*, *firewall*, NAT, atau mekanisme *failover*, kemudian rancangan diuji kembali hingga sesuai.

Hasil Pengujian Segmentasi VLAN, DHCP, dan Konektivitas

Pengujian dilakukan pada setiap segmen VLAN menggunakan *endpoint* berbasis Linux ringan pada GNS3. Setiap *endpoint* diuji untuk memperoleh IP Address secara otomatis melalui DHCP, memverifikasi *gateway*, melakukan ping ke *gateway* VLAN, dan mengakses internet simulasi ke alamat 8.8.8.8, serta diverifikasi melalui DHCP lease pada R-Mikrotik-*Gateway*. Rangkuman hasil pengujian keempat VLAN ditunjukkan pada Tabel 4.

Tabel 4. Hasil Pengujian Segmentasi VLAN, DHCP, dan Konektivitas.

Segmen VLAN	IP Address (DHCP)	*Gateway*	Ping *Gateway*	Akses Internet (8.8.8.8)	DHCP Lease
VLAN 30 CCTV	192.168.30.253	192.168.30.1	0% *packet loss*	0% *packet loss*	bound
VLAN 10 Admin	192.168.10.254	192.168.10.1	0% *packet loss*	0% *packet loss*	bound
VLAN 20 Operasional	192.168.20.254	192.168.20.1	0% *packet loss*	0% *packet loss*	bound
VLAN 40 Guest WiFi	192.168.40.254	192.168.40.1	0% *packet loss*	0% *packet loss*	bound

Tabel 4 menunjukkan bahwa seluruh *endpoint* berhasil memperoleh IP Address secara otomatis sesuai network VLAN masing-masing melalui DHCP server pada R-Mikrotik-*Gateway*. *Endpoint* CCTV/NVR pada VLAN 30 memperoleh 192.168.30.253, *Client*-Admin-Laptop pada VLAN 10 memperoleh 192.168.10.254, *Client*-Operasional-Laptop pada VLAN 20 memperoleh 192.168.20.254, dan *Client*-Guest-LaptopWifi pada VLAN 40 memperoleh 192.168.40.254, seluruhnya dengan *subnet mask* 255.255.255.0. Setiap *client* juga menerima informasi *gateway* yang sesuai dan berhasil melakukan ping ke *gateway* VLAN masing-masing dengan hasil 0% *packet loss*. Pengujian akses internet pada VLAN 10, 20, dan 40 berhasil menjangkau alamat 8.8.8.8 dengan 0% *packet loss*, yang membuktikan bahwa fungsi *routing* dan NAT pada *router* telah berjalan; sementara pada VLAN 30 CCTV pengujian diverifikasi hingga *gateway* sesuai fungsi segmennya. Seluruh alamat IP tersebut juga tercatat berstatus bound pada tabel DHCP lease *router*, sehingga membuktikan bahwa konfigurasi access VLAN pada *switch* distribusi, *trunk* VLAN pada *switch* core, serta *interface* VLAN dan DHCP server pada *router* telah berjalan sesuai rancangan.

Hasil Pengujian Failover dan Failback Multi-ISP

Pengujian *failover* dan *failback* dilakukan menggunakan *Client*-Operasional-Laptop karena mekanisme perpindahan jalur bekerja pada R-Mikrotik-*Gateway*, bukan pada masing-masing *endpoint*. Koneksi utama menggunakan ISP1-MyEnterprise dan koneksi cadangan menggunakan ISP2-Starlink. Pengujian dilakukan dengan melakukan ping menuju alamat 8.8.8.8 pada tiga kondisi, yaitu kondisi normal, kondisi ISP1 dinonaktifkan (*failover*), dan kondisi ISP1 diaktifkan kembali (*failback*), dengan hasil pada Tabel 5.

Tabel 5. Hasil Pengujian *Failover* dan *Failback Multi-ISP*.

Kondisi	Route ISP1 (10.10.10.1)	Route ISP2 (20.20.20.1)	Ping ke 8.8.8.8
Normal (sebelum *failover*)	Aktif — flag As, distance 1	Cadangan — flag s, distance 2	0% *packet loss*
ISP1 dinonaktifkan (*failover*)	Nonaktif — flag Is	Aktif — flag As	0% *packet loss*
ISP1 aktif kembali (*failback*)	Aktif — flag As, distance 1	Cadangan — flag s, distance 2	0% *packet loss*

Tabel 5 menunjukkan bahwa pada kondisi normal, *default route* menuju ISP1-MyEnterprise memiliki flag As dengan distance 1 sehingga menjadi jalur utama, sedangkan route menuju ISP2-Starlink berada sebagai cadangan dengan flag s dan distance 2. Ketika ISP1 dinonaktifkan, route ISP1 berubah menjadi Is (tidak aktif) dan route ISP2 berubah menjadi As, sehingga R-Mikrotik-*Gateway* secara otomatis mengalihkan trafik internet ke jalur cadangan; pada kondisi ini *client* tetap berhasil melakukan ping ke 8.8.8.8 dengan 0% *packet loss*. Setelah ISP1 diaktifkan kembali, route ISP1 kembali menjadi As dengan distance 1 dan digunakan sebagai jalur utama, sementara ISP2 kembali menjadi cadangan, dengan *client* tetap memperoleh 0% *packet loss*. Hasil ini membuktikan bahwa mekanisme *failover* dan *failback* berjalan sesuai rancangan berdasarkan prioritas distance *routing*.

Hasil Pengujian Firewall Jaringan Guest

Pengujian *firewall* dilakukan untuk memastikan bahwa *Client*-Guest-LaptopWifi pada VLAN 40 tetap dapat mengakses internet, tetapi tidak dapat menjangkau jaringan internal yang meliputi VLAN 10 Admin, VLAN 20 Operasional, dan VLAN 30 CCTV. Hasil pengujian ditunjukkan pada Tabel 6.

Tabel 6. Hasil Pengujian *Firewall* Jaringan Guest (VLAN 40).

Pengujian dari *Client*-Guest	Tujuan	Hasil	Keterangan
Ping ke internet (8.8.8.8)	Internet simulasi	0% *packet loss*	Diizinkan
Ping ke *Client*-Admin (VLAN 10)	192.168.10.254	100% *packet loss*	Diblokir
Ping ke *Client*-Operasional (VLAN 20)	192.168.20.254	100% *packet loss*	Diblokir
Ping ke *Endpoint*-CCTV/NVR (VLAN 30)	192.168.30.253	100% *packet loss*	Diblokir

Tabel 6 memperlihatkan bahwa *Client*-Guest-LaptopWifi berhasil melakukan ping ke alamat 8.8.8.8 dengan 0% *packet loss*, sehingga jaringan Guest tetap dapat mengakses internet melalui R-Mikrotik-*Gateway* dan ISP1-MyEnterprise. Sebaliknya, seluruh pengujian ping dari *Client*-Guest menuju perangkat pada jaringan internal, yaitu *Client*-Admin pada VLAN 10, *Client*-Operasional pada VLAN 20, dan *Endpoint*-CCTV/NVR pada VLAN 30, menghasilkan 100% *packet loss*. Hal ini membuktikan bahwa rule *firewall* pada R-Mikrotik-*Gateway* berhasil

memblokir akses dari VLAN 40 Guest menuju seluruh segmen internal, sehingga jaringan internal termasuk sistem pengawasan CCTV tetap terlindungi. Dengan demikian, konfigurasi *firewall* telah berjalan sesuai rancangan keamanan jaringan, yaitu mengizinkan akses internet bagi tamu tanpa membuka akses ke jaringan internal perusahaan.

Pembahasan

Hasil pengujian menunjukkan bahwa rancangan jaringan berhasil memisahkan lalu lintas data berdasarkan fungsi melalui segmentasi VLAN, yaitu Admin, Operasional, CCTV, dan Guest WiFi. Setiap *client* memperoleh IP Address sesuai network VLAN masing-masing secara otomatis melalui DHCP dan terhubung ke *gateway* dengan hasil 0% *packet loss*. Temuan ini sejalan dengan penelitian yang menegaskan bahwa penerapan VLAN mampu mengurangi *broadcast domain* dan memperkuat keamanan melalui pemisahan trafik (Ajiji et al., 2021). Skema pengalamatan IP yang terstruktur juga mempermudah pengelolaan perangkat dan mengurangi potensi konflik alamat, konsisten dengan hasil perancangan jaringan berbasis VLAN dan NDLC pada lingkungan sekolah maupun perkantoran (Setiawan et al., 2024).

Pada aspek ketersediaan internet, mekanisme *multi-ISP* berbasis *failover* dan *failback* berhasil direpresentasikan pada R-Mikrotik-*Gateway*. Ketika jalur utama ISP1-MyEnterprise dinonaktifkan, *default route* secara otomatis beralih ke ISP2-Starlink sehingga *client* tetap dapat mengakses internet dengan 0% *packet loss*; ketika ISP1 aktif kembali, koneksi kembali menggunakan jalur utama sesuai prioritas distance *routing*. Hasil ini memperkuat temuan bahwa pemanfaatan dua ISP dengan mekanisme *failover* mampu menjaga kontinuitas layanan jaringan (Amalia et al., 2023). Pendekatan serupa pada jaringan dual ISP berbasis MikroTik dan GNS3 juga terbukti meningkatkan ketersediaan koneksi (Andra et al., 2026). Optimalisasi mekanisme *failover* bahkan dapat dilakukan lebih lanjut untuk menjaga *uptime* jaringan (Hoesiin & Yuliandi, 2025).

Pengujian *firewall* membuktikan bahwa jaringan Guest pada VLAN 40 tetap dapat mengakses internet, namun tidak dapat menjangkau jaringan internal Admin, Operasional, maupun CCTV, yang ditunjukkan dengan hasil 100% *packet loss* pada seluruh pengujian menuju segmen internal. Hal ini menegaskan bahwa kontrol akses berbasis *firewall* dan segmentasi VLAN mampu meningkatkan keamanan jaringan tanpa menghilangkan fleksibilitas komunikasi yang diperlukan, sebagaimana ditekankan pada penerapan *inter-VLAN routing* di jaringan korporat (Abdelhalim et al., 2020). Penggunaan policy *routing* dan *failover* pada *router* MikroTik juga sejalan dengan praktik pengelolaan jalur akses internet yang efisien (Pambudi & Muslim, 2017). Secara keseluruhan, penerapan metode NDLC menghasilkan

rancangan jaringan *wireline* dan *wireless* yang lebih terstruktur, aman, dan siap dikembangkan sesuai kebutuhan operasional perusahaan (Prasetyo et al., 2025).

5. KESIMPULAN DAN SARAN

Berdasarkan hasil perancangan, simulasi, dan pengujian, penelitian ini berhasil menghasilkan rancangan jaringan *wireline* dan *wireless* yang lebih terstruktur untuk mendukung pengembangan kantor dari satu ruko menjadi dua ruko menggunakan metode *Network Development Life Cycle* (NDLC). Skema pengalamatan IP dirancang secara terstruktur berdasarkan segmentasi VLAN 10 Admin, VLAN 20 Operasional, VLAN 30 CCTV, dan VLAN 40 Guest WiFi, sehingga setiap *client* memperoleh IP sesuai VLAN, terhubung ke *gateway*, dan dapat mengakses internet dengan hasil 0% *packet loss*. Penerapan *firewall* berhasil membatasi jaringan Guest agar tidak dapat mengakses jaringan internal, sementara mekanisme *multi-ISP* berbasis *failover* dan *failback* berhasil mengalihkan koneksi ke ISP cadangan ketika jalur utama dinonaktifkan dan mengembalikannya ketika jalur utama aktif kembali. Dengan demikian, rancangan jaringan yang dihasilkan telah sesuai dengan tujuan penelitian dan dapat menjadi acuan pengembangan infrastruktur jaringan perusahaan secara bertahap. Penelitian selanjutnya disarankan menerapkan rancangan pada perangkat fisik serta menambahkan pengujian performa jaringan, *load balancing*, dan keamanan tingkat lanjut agar kualitas jaringan dapat dianalisis secara lebih mendalam.

DAFTAR REFERENSI

Abdelhalim, A., et al. (2020). Implementation of VLAN and inter-VLAN in corporate networks. *International Journal of Advanced Research (IJAR).*

Ajiji, Y. M., et al. (2021). Network performance through virtual local area network (VLAN) implementation and enforcement on network security for enterprise. *International Journal of Advanced Networking and Applications*, *12*(6), 4750–4762. https://doi.org/10.35444/IJANA.2021.12604

Amalia, E. R., Nurheki, Saputra, R., Ramadhana, C., & Yossy, E. H. (2023). Computer network design and implementation using load balancing technique with *Per Connection Classifier* (PCC) method based on MikroTik router. *CoMBInES: Conference on Management, Business, Innovation, Education and Social Sciences.* https://doi.org/10.1016/j.procs.2022.12.116

Andra, A. Y., Mooduto, H. A., Sukma, F., & Amnur, H. (2026). Layanan internet service provider dengan GNS3 menggunakan Mikrotik dan Debian pada jaringan dual ISP. *JITSI: Jurnal Ilmiah Teknologi Sistem Informasi*, *7*(1), 19–26. https://doi.org/10.62527/jitsi.7.1.552

Azmi, K., Syamsul, S., & Fakhrurrazi, F. (2022). Studi penggunaan dua ISP dengan *load balancing* dan *failover* untuk meningkatkan kinerja jaringan berbasis router MikroTik. *Jurnal TEKTRO, 6*(2).

Hayati, I., & Kurniawan, M. T. (2016). Perancangan infrastruktur LAN pada Yayasan Kesehatan (Yakes) Telkom Bandung dengan model Cisco *three-layer hierarchical* menggunakan metodologi *Network Development Life Cycle* (NDLC). *JRSI: Jurnal Rekayasa Sistem dan Industri, 3*(4). https://doi.org/10.25124/jrsi.v3i04.278

Hoesiin, & Yuliandi, B. (2025). Optimizing network uptime through dual ISP failover implementation using Netwatch. *Journal Informatic, Education and Management (JIEM), 7*(2), 336–349. https://doi.org/10.61992/jiem.v7i2.150

Nourildean, S. W., Mohammed, Y. A., & Attallah, H. A. (2023). Virtual local area network performance improvement using ad hoc routing protocols in a wireless network. *Computers, 12*(2), Article 28. https://doi.org/10.3390/computers12020028

Pambudi, R., & Muslim, M. A. (2017). Implementasi *policy-based routing* dan *failover* menggunakan router MikroTik untuk membagi jalur akses internet di FMIPA Unnes. *Jurnal Teknologi dan Sistem Komputer, 5*(2), 57–61. https://doi.org/10.14710/jtsiskom.5.2.2017.57-61

Prasetyo, F. H. P., Infitharina, E., & Febriyansyah, M. (2025). Penerapan metode *Network Development Life Cycle* (NDLC) dalam pengembangan jaringan komputer. *Journal of Informatics and Communication Technology (JICT), 7*(1), 80–87. https://doi.org/10.52661/jict.v7i1.410

Prasetyo, S. E., & Cung, J. (2022). *Analysis of network load balancing implementation.* Universitas Internasional Batam.

Setiawan, R., Duskarnaen, M. F., & Ajie, H. (2024). Perancangan jaringan VLAN (*Virtual Local Area Network*) di SMKN 40 Jakarta dengan menggunakan metode *Network Development Life Cycle* (NDLC). *PINTER: Jurnal Pendidikan Teknik Informatika dan Komputer, 8*(1). https://doi.org/10.21009/pinter.8.1.5

Sofana, I. (2016). *Membangun jaringan komputer.* Informatika.

Stallings, W. (2020). *Data and computer communications* (11th ed.). Pearson.

Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer networks* (5th ed.). Pearson.