Volume 7 Nomor 1 Edisi Agustus 2025
E-ISSN: **2714-8599**

PERANCANGAN DAN IMPLEMENTASI INFRASTRUKTUR JARINGAN DI PT CEMARA INTAN SHIPYARD

Sherly, Haeruddin, Gautama Wijaya
Universitas Internasional Batam
Email korespondensi: 2232028.sherly@uib.edu

Abstrak

Konfigurasi yang kurang optimal untuk penggunaan dua jalur koneksi internet dari Solnet dengan bandwidth 15 Mbps (ISP1) dan 10 Mbps (ISP2) menyebabkan permasalahan pada penentuan gateway default untuk trafik jaringan. Hal ini membuat koneksi internet tidak stabil dan pengguna mengalami fluktuasi kecepatan internet. Metode PPDIOO digunakan sebagai pendekatan perancangan jaringan, yaitu Prepare, Plan, Design, Implementation, Operate, dan Optimize. Penyelesaian masalah dilakukan melalui penerapan metode PPDIOO, penambahan core router, penerapan VLAN untuk segmentasi jaringan, pengaturan rute trafik yang tepat, serta penambahan aturan firewall untuk memblokir situs. Dengan pengelompokan lalu lintas berdasarkan divisi perusahaan, lalu lintas jaringan dapat dikelola dengan lebih efektif, serta memungkinkan pengaturan prioritas lalu lintas yang sesuai dengan kebutuhan. Hasilnya adalah konektivitas internet perusahaan kini lebih stabil, andal, dan aman. Penelitian selanjutnya dapat berfokus pada pengembangan dan penerapan solusi failover internet yang lebih andal secara otomatis dengan memanfaatkan koneksi dari penyedia layanan internet (ISP) yang berbeda. Langkah ini penting untuk menciptakan redundansi infrastruktur yang nyata dan mengurangi risiko downtime akibat hanya mengandalkan satu provider.

Abstract

The suboptimal setup for utilizing two internet connections paths from Solnet, with bandwidth of 15 Mbps (ISP1) and 10 Mbps (ISP2), leads to issues in determining the default gateway for network traffic. As a result, the internet connection becomes unstable, and users face inconsistent internet speeds. The PPDIOO technique, which stands for Prepare, Plan, Design, Implementation, Operate, and Optimize, is used as the network design methodology. Problem solving is done through the application of the PPDIOO method, adding a core router, applying VLANs for network segmentation, setting the right traffic routes, and adding firewall rules to block sites. By grouping traffic based on company divisions, network traffic can be managed more effectively, as well as enabling customized traffic prioritization. As a result, the company's internet connectivity is now more stable, reliable and secure. Future research could focus on developing and implementing a more reliable internet failover solution that automatically utilizes connections from different internet service providers (ISPs). This step is important to create real infrastructure redundancy and reduce the risk of downtime due to relying on only one provider.

Keywords: *network, internet, VLAN, traffic, PPDIOO*

Pendahuluan

Di era digital saat ini, teknologi informasi menjadi semakin penting untuk mendukung operasional perusahaan dengan lebih efisien (Wijoyo et al., 2023). Fondasi utama untuk memproses serta mendistribusikan data dan informasi adalah infrastruktur TI, yang terdiri dari perangkat keras seperti komputer, server, dan perangkat jaringan. Di dalamnya, terdapat jaringan komputer yang memiliki peran penting untuk memfasilitasi pertukaran data dan komunikasi antar perangkat dalam perusahaan. Infrastruktur ini mencakup perangkat seperti switch dan router serta protokol jaringan yang digunakan untuk mengatur lalu lintas data secara efisien dan aman. Keandalan sistem jaringan sangat krusial untuk memastikan operasional perusahaan berjalan dengan lancar (Ramadhan et al., 2024).

Dalam implementasi jaringan komputer, terdapat berbagai tantangan dan masalah yang dapat terjadi, seperti hambatan komunikasi berupa time-out, risiko keamanan, keterlambatan pengiriman data sehingga data gagal mencapai tujuan, serta kerusakan data. Hal ini dapat diatasi dengan menggunakan perangkat jaringan seperti router yang memainkan peran penting dalam mengatur jalur lalu lintas data agar pengiriman data dapat berlangsung dengan baik dan tepat sasaran. Router yang dapat mengelola jalur data dan mengoptimalkan distribusi koneksi menyelesaikan berbagai masalah jaringan, memungkinkan komunikasi dalam sistem jaringan perusahaan berjalan secara stabil (Antoro, 2014).

Demi mendukung operasional perusahaan yang lebih fokus dan stabil, firewall Layer 7 dapat diterapkan untuk memfilter dan memblokir akses ke situs web atau aplikasi tertentu. Dengan penerapan pada perangkat seperti MikroTik RouterOS melalui fitur regex (regular expression), perusahaan dapat mengendalikan akses internet yang sehat. Ini secara efektif memblokir akses ke situs negatif dan media sosial yang mengganggu produktivitas karyawan (Ramadhani et al., 2025). Selain itu, keamanan jaringan juga dapat diperkuat dengan penerapan VLAN yang memisahkan lalu lintas ke segmen-segmen berbeda, sehingga membatasi akses yang tidak relevan dan mengurangi potensi ancaman (Umah et al., 2025).

Firewall Mangle pada MikroTik RouterOS adalah fitur penting dalam pengelolaan lalu lintas data jaringan secara efisien. Salah satu fungsinya adalah Mark Routing, suatu mekanisme yang memungkinkan pemilihan jalur paket data secara selektif berdasarkan tanda (mark) tertentu. Dengan memanfaatkan fitur ini, lalu lintas jaringan dapat diarahkan melalui jalur koneksi yang berbeda, sehingga penggunaan bandwidth menjadi lebih seimbang dan stabilitas koneksi jaringan dapat meningkat (Hamza, 2022).

Penelitian oleh Octaviyana dan Soewito (2023) membahas perancangan ulang jaringan institusi dengan menerapkan kerangka kerja PPDIOO dari Cisco. Penelitian ini menunjukkan bahwa metode PPDIOO adalah pendekatan yang sistematis dan komprehensif dalam menangani masalah kualitas layanan

jaringan, seperti kurangnya pengelolaan bandwidth dan sistem pemantauan di sebuah institusi kesehatan. Topologi yang dirancang mencakup tiga router ISP, satu load balancer, switch inti dan distribusi, serta sistem pemantauan jaringan. Dalam pelaksanaannya, penelitian ini menggunakan perangkat MikroTik RouterBOARD untuk pengelolaan bandwidth serta alat pemantauan jaringan berupa Grafana untuk memastikan penggunaan sumber daya yang optimal. Hasil penelitian ini lebih lanjut menekankan efektivitas PPDIOO, yang mampu menghasilkan jaringan dengan topologi yang lebih optimal dan memungkinkan pengukuran kinerja secara langsung (Octaviyana & Soewito, 2023).

Selain itu, penelitian oleh Aren Brayen Sangi et al. (2023) membahas perancangan dan implementasi jaringan internet berbasis MikroTik di SMP Negeri 3 Tondano. Tujuan dari penelitian ini adalah untuk meningkatkan kualitas jaringan internet yang sebelumnya memiliki jangkauan terbatas, sehingga dapat memberikan koneksi yang lebih stabil dan aman bagi siswa maupun staf. Proses pelaksanaan jaringan mencakup konfigurasi dasar router MikroTik, pengaturan DHCP, IP address, DNS, firewall, dan hotspot untuk mengatur akses internet. Selain itu, sistem keamanan juga diterapkan, seperti penetapan password pada setiap Wi-Fi untuk mencegah penyalahgunaan internet. Setelah jaringan diimplementasikan, dilakukan pemantauan dan pengelolaan rutin untuk memastikan stabilitas sistem. Hasil dari pelaksanaan ini adalah jaringan internet yang lebih stabil dan mudah diakses oleh seluruh warga sekolah (Sangi et al., 2023).

Kegiatan yang dilakukan oleh penulis adalah mengatasi masalah kestabilan internet di lingkungan perusahaan dengan penerapan VLAN untuk memisahkan segmen jaringan dan pengaturan rute trafik. Tujuan dari pelaksanaan kegiatan ini adalah untuk memberikan kontribusi nyata terhadap perusahaan dengan meningkatkan efisiensi infrastruktur jaringan yang digunakan sehingga memenuhi kebutuhan akan akses internet yang stabil, aman, dan dapat diandalkan untuk mendukung aktivitas harian, seperti kegiatan operasional, administrasi, dan komunikasi.

Masalah

Permasalahan utama yang dihadapi oleh PT Cemara Intan Shipyard adalah ketidakstabilan jaringan akibat konfigurasi yang kurang optimal. Perusahaan ini menggunakan dua jalur koneksi internet dari Solnet dengan bandwidth 15 Mbps (ISP1) dan 10 Mbps (ISP2). Namun, kedua koneksi tersebut digabungkan ke dalam satu switch tanpa adanya konfigurasi lebih lanjut. Hal ini menyebabkan permasalahan pada penentuan gateway default untuk trafik jaringan sehingga koneksi internet tidak konsisten. Beberapa pengguna mengeluhkan fluktuasi kecepatan internet, yang terkadang dapat berjalan dengan cepat dan sangat lambat hingga Request Timed Out (RTO). Ketidakstabilan ini membuat pekerjaan yang membutuhkan internet menjadi terhambat.

Metode

Dalam kegiatan ini, metode PPDIOO digunakan sebagai pendekatan perancangan jaringan. Metode PPDIOO terdiri dari enam tahapan, yaitu Prepare, Plan, Design, Implementation, Operate, dan Optimize (Br Sipayung et al., 2024). Metode PPDIOO dikembangkan oleh Cisco untuk mendukung pengembangan jaringan. Keuntungan utama dari penggunaan metode PPDIOO adalah untuk mengurangi TCO (Total Cost of Ownership). Selain itu, PPDIOO juga meningkatkan ketersediaan jaringan melalui penerapan validasi operasi jaringan dengan desain yang solid (Yuliana & Mogi, 2020). Berikut adalah gambar dari tahapan metode PPDIOO (Habibullah et al., 2022).

Gambar 1. Siklus PPDIOO

Siklus PPDIOO terbagi menjadi tiga kelompok besar, yaitu tahapan awal pelaksanaan (prepare), tahapan pelaksanaan kegiatan (plan, design, implement, dan operate), serta tahapan akhir (optimize). Tahapan awal pelaksanaan dimulai dengan tahap prepare (persiapan). Pada tahap ini dilakukan penilaian terhadap kebutuhan organisasi dan menganalisis jaringan yang sudah ada untuk mendapatkan pemahaman yang mendalam tentang konteks dan kebutuhan sistem jaringan yang akan dibangun (Br Sipayung et al., 2024). Metode pengumpulan data yang diterapkan dalam kegiatan ini adalah melalui observasi langsung dan wawancara dengan pembimbing lapangan di tempat magang. Pemilihan metode ini didasarkan pada pentingnya mendapatkan informasi secara menyeluruh, baik dari aspek teknis maupun pengalaman nyata yang dimiliki oleh perusahaan. Wawancara dilakukan untuk mendapatkan informasi awal mengenai kondisi infrastruktur jaringan dan masalah yang sering muncul.

Setelah memperoleh informasi awal, dilakukan observasi langsung di lokasi untuk menyesuaikan informasi tersebut dengan keadaan nyata. Hal ini mencakup pemeriksaan langsung terhadap perangkat jaringan, penelusuran jalur koneksi jaringan, serta pemantauan sistem yang sedang beroperasi. Data yang dihasilkan dari wawancara dan observasi selanjutnya dianalisis untuk memahami masalah dan menentukan langkah penyelesaian yang tepat. Dengan pendekatan ini, solusi yang dirancang akan lebih sesuai dan relevan dengan kebutuhan di lapangan.

Tahapan pelaksanaan kegiatan dimulai dengan tahap plan (perencanaan). Pada tahap ini kebutuhan mulai ditentukan. Tahap design (perancangan) fokus pada perancangan topologi dan arsitektur jaringan. Tahap implementation (implementasi) dilakukan dengan mengubah rancangan menjadi sistem nyata melalui pemasangan dan konfigurasi perangkat jaringan sesuai dengan spesifikasi yang sudah dirancang. Pada tahap operate (operasional) dilakukan pengujian dan pemeliharaan jaringan yang telah

diinstal. Pemantauan dilakukan untuk memastikan sistem beroperasi dengan baik, serta melakukan perbaikan jika ada masalah (Br Sipayung et al., 2024).

Pada tahap akhir kegiatan, tahap optimize (optimalisasi) dilakukan untuk terus meningkatkan kualitas jaringan. Evaluasi dilakukan secara berkelanjutan untuk menemukan peluang perbaikan dari segi efisiensi, keamanan, dan perkembangan teknologi jaringan agar sistem yang diterapkan semakin optimal (Br Sipayung et al., 2024). Evaluasi ini meliputi pemeriksaan terhadap konfigurasi yang diterapkan, kinerja performa setelah adanya perubahan, serta stabilitas keseluruhan sistem. Selain itu, dilakukan wawancara kepada pengguna untuk memastikan dampak positif yang diperoleh setelah konfigurasi ulang jaringan.

Berikut merupakan jadwal dan anggaran pelaksanaan kegiatan di PT Cemara Intan Shipyard.

Kegiatan	Feb			Mar				Apr				Mei				Jun	
Persiapan (Wawancara dan Observasi)																	
Perencanaan (Menentukan kebutuhan)																	
Desain (Rancang Jaringan)																	
Implementasi (Konfigurasi)																	
Operasional (Monitoring)																	
Optimalisasi (Evaluasi)																	
Laporan																	

Tabel 1. Jadwal Pelaksanaan Kegiatan

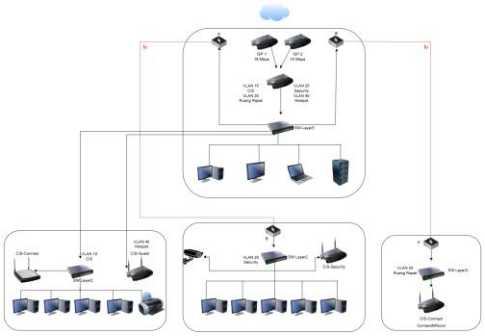
No	Rancangan Aktivitas	Jenis Anggaran	Volume	Unit	Satuan	Jumlah
1	Observasi dan wawancara	Biaya Konsumsi	15	kali	Rp 50.000	Rp 750.000
		Biaya Transportasi	15	kali	Rp 12.000	Rp 180.000
		Biaya Koneksi Internet	1	paket	Rp 60.000	Rp 60.000
2	Perancangan Luaran	Router	1	unit	Rp 935.000	Rp 935.000
		Switch Manageable	1	unit	Rp 2.500.000	Rp 2.500.000
		Kabel LAN	1	paket	Rp 2.065.500	Rp 2.065.500
		Kabel FO 4 core outdoor (1000M)	1	paket	Rp 1.550.000	Rp 1.550.000
		OTB 24 core	1	unit	Rp 350.000	Rp 350.000
3	Pendampingan Implementasi Luaran	Biaya Transportasi	15	kali	Rp 12.000	Rp 180.000
		Biaya Koneksi Internet	1	paket	Rp 60.000	Rp 60.000
4	Pembuatan laporan	Materai	2	Eksemplar	Rp 12.000	Rp 24.000
TOTAL ANGGARAN						**Rp 8.654.500**

Tabel 2. Anggaran Pelaksanaan Kegiatan

Pembahasan

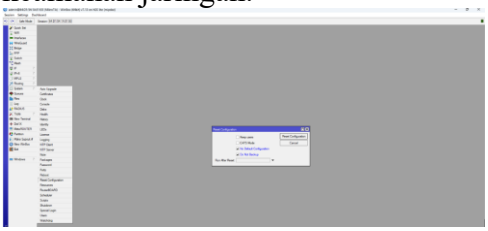
Pada tahap persiapan dilakukan observasi dan wawancara terkait infrastruktur jaringan yang ada. Perangkat jaringan ditinjau untuk mengetahui kondisi yang terjadi dan memeriksa pengaturan yang telah dikonfigurasi sebelumnya. Hal ini bertujuan untuk memahami masalah dan menentukan solusi yang tepat. Masalah ditemukan pada pengaturan jaringan yang kurang optimal sehingga mempengaruhi kestabilan koneksi internet. Untuk mengatasi masalah yang telah diidentifikasi sebelumnya, dilakukan perencanaan untuk menambahkan satu unit router sebagai router utama untuk mengatasi masalah ini. Penulis ikut serta dalam melakukan perencanaan untuk desain ulang jaringan dan implementasi jaringan baru dengan konfigurasi ulang perangkat jaringan, mempertimbangkan pembagian VLAN yang tepat, pengaturan IP, dan konektivitas antar perangkat untuk mendukung operasional perusahaan. Solusi ini bertujuan untuk membagi jalur koneksi internet menjadi beberapa VLAN untuk memastikan pembagian bandwidth yang lebih optimal, menerapkan kebijakan routing agar trafik dari setiap VLAN dapat diarahkan ke ISP yang sesuai,

membuat firewall rules dasar untuk block situs tertentu, serta menambahkan aturan firewall untuk NAT dan traffic marking agar jalur routing mengikuti ISP yang telah ditentukan.



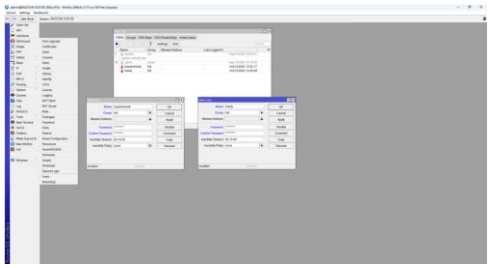
Gambar 2. Desain Jaringan

Desain jaringan dirancang untuk memenuhi kebutuhan penggunaan internet di area perusahaan. Diagram ini menunjukkan pembagian VLAN untuk masing-masing fungsi, yaitu VLAN10 untuk area office, VLAN20 untuk departemen security, VLAN30 untuk ruang rapat, dan VLAN40 untuk hotspot tamu. Setiap komponen desain ini dirancang untuk mengoptimalkan kinerja dan keamanan jaringan.



Gambar 3. Reset Mikrotik

Proses implementasi diawali dengan mereset konfigurasi Mikrotik. Reset ini bertujuan untuk menghapus semua pengaturan bawaan pada router dan mulai konfigurasi dari awal dengan pengaturan yang baru. Hal ini sangat penting untuk mencegah terjadinya konflik pengaturan atau konfigurasi yang tidak diperlukan.



Gambar 4. Manajemen User

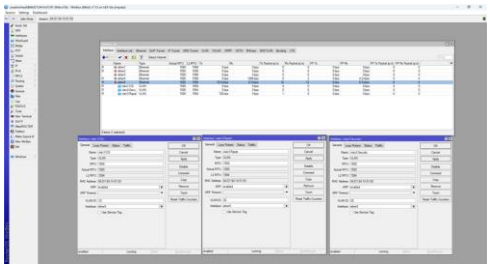
Setelah proses reset selesai, tahap berikutnya adalah membuat user baru. Hal ini bertujuan untuk memperkuat keamanan jaringan, terutama untuk menghindari penggunaan user default 'admin' yang seringkali menjadi sasaran serangan. Pada tahap ini, user baru ditambahkan dengan hak akses penuh dan user 'admin' dinonaktifkan.

Setelah user baru dibuat, alamat IP ditambahkan pada setiap interface fisik yang ada di perangkat Mikrotik, mulai dari ether1 hingga ether5. Alamat IP berfungsi sebagai identitas setiap interface yang akan terhubung ke jaringan atau perangkat tertentu.

Address	Network	Interface
private	*private*	ether1
private	*private*	ether2
192.168.33.1/24	192.168.33.0	ether3
192.168.44.1/24	192.168.44.0	ether4
192.168.55.1/24	192.168.55.0	ether5

Tabel 3. Alamat IP Interface

Ether1 dihubungkan ke ISP1 dan Ether2 dihubungkan ke ISP2. Ether3 dan Ether4 digunakan untuk jaringan lokal. Ether5 berfungsi sebagai gateway untuk jaringan VLAN. Penambahan alamat IP pada interface ether ini bertujuan untuk memisahkan jalur komunikasi antar jaringan dan untuk mengarahkan trafik melalui firewall dan routing.



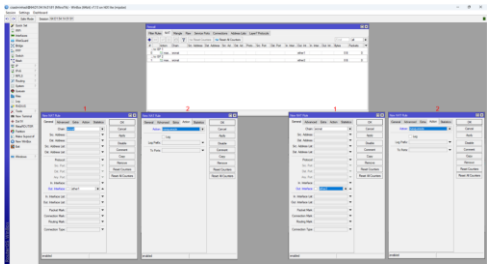
Gambar 5. Pembuatan VLAN

VLAN dikonfigurasikan pada interface ether5 untuk memecah jaringan menjadi beberapa segmen sesuai dengan departemen yang ada di perusahaan. Hal ini dilakukan untuk meningkatkan aspek keamanan, memisahkan lalu lintas antar departemen, dan mempermudah manajemen jaringan. VLAN1-CIS (VLAN ID 10) dialokasikan untuk bagian office dan akan berfungsi sebagai jaringan utama yang diakses oleh karyawan untuk aktivitas sehari-hari. VLAN2-Security (VLAN ID 20) dialokasikan untuk departemen security. VLAN3-Rapat (VLAN ID 30) dialokasikan untuk ruang rapat.

Address	Network	Interface
192.168.50.1/24	192.168.50.0	vlan1-CIS
192.168.113.1/24	192.168.113.0	vlan2-Security
192.168.114.1/24	192.168.114.0	vlan3-Rapat
192.168.200.1/24	192.168.200.0	vlan4-Hotspot

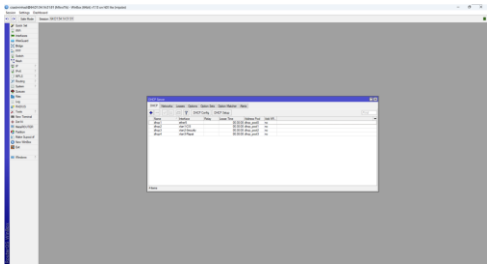
Tabel 4. Alamat IP VLAN

Setelah pembuatan VLAN-VLAN ini, setiap VLAN diberi alamat IP. Dengan struktur pembagian alamat IP yang jelas, pengelolaan jaringan menjadi lebih mudah dan pengaturan lalu lintas data antara VLAN dapat dilakukan dengan lebih efektif.



Gambar 6. Konfigurasi NAT

Selanjutnya, pengaturan NAT (Network Address Translation) dilakukan untuk memungkinkan perangkat di jaringan lokal dapat mengakses internet. Dalam pengaturan ini, NAT dikonfigurasi dengan metode masquerade. Aturan NAT dibuat dengan chain srcnat dan out-interface ether1 yang terhubung ke ISP1 serta ether2 yang terhubung ke ISP2. Dengan pengaturan ini, semua lalu lintas yang keluar dari jaringan internal ke internet melalui ISP1 dan ISP2 akan "disamarkan" menggunakan alamat IP publik yang disediakan oleh ISP.

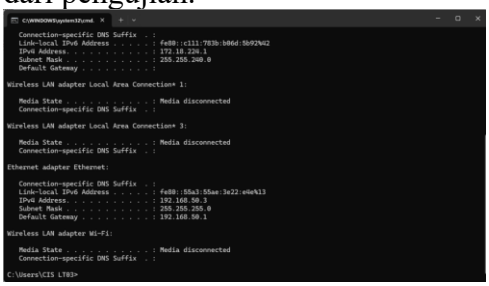


Gambar 7. DHCP Server

DHCP server dikonfigurasi pada Mikrotik untuk membantu mengelola alamat IP di jaringan dan bertugas untuk memberikan alamat IP secara otomatis kepada perangkat yang terhubung ke jaringan. Dengan melakukan konfigurasi DHCP server pada beberapa interface, seperti ether5, VLAN1, VLAN2, dan VLAN3, perangkat yang terhubung melalui switch layer 3 atau langsung ke ether5 dapat mendapatkan alamat

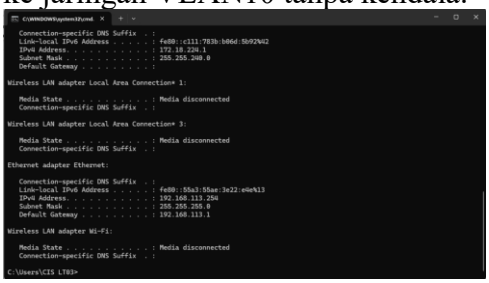
IP secara otomatis tanpa perlu pengaturan manual.

Setelah menyelesaikan konfigurasi DHCP, pengujian dilakukan dengan kabel LAN yang dicolokkan ke switch layer 3. Pengujian dilakukan secara bergantian untuk memastikan bahwa semua VLAN dan interface ether5 beroperasi dengan baik. Untuk memastikan apakah perangkat memperoleh alamat IP yang benar dari DHCP server, perintah "ipconfig" dijalankan pada komputer yang terhubung. Berikut adalah hasil dari pengujian.



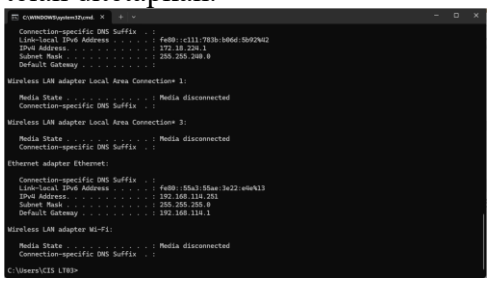
Gambar 8. Pengujian VLAN1

Hasil menunjukkan bahwa perangkat menerima alamat IP dari subnet VLAN10. Alamat IP yang didapatkan adalah 192.168.50.3 dengan gateway 192.168.50.1. Dari hasil tersebut, dapat disimpulkan bahwa konfigurasi DHCP server untuk VLAN10 berfungsi dengan baik, dan perangkat dapat terhubung ke jaringan VLAN10 tanpa kendala.



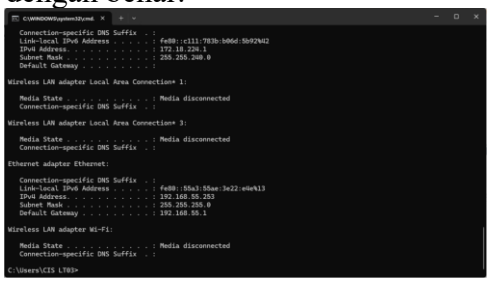
Gambar 9. Pengujian VLAN2

Berdasarkan hasil pengujian, perangkat juga menerima alamat IP dari subnet VLAN20. Alamat IP yang didapatkan adalah 192.168.113.254 dan gateway 192.168.113.1. Ini menunjukkan bahwa perangkat dapat berkomunikasi dalam jaringan VLAN20 dengan konfigurasi yang telah ditetapkan.



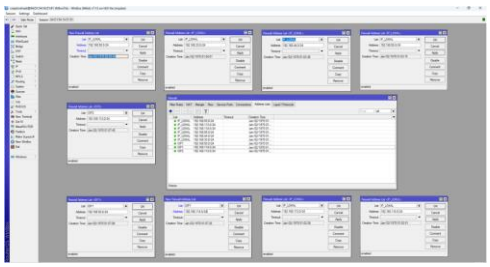
Gambar 10. Pengujian VLAN3

Pengujian konektivitas VLAN30 menunjukkan bahwa perangkat menerima alamat IP dari subnet VLAN30. Alamat IP yang diperoleh adalah 192.168.114.251 dan gateway 192.168.114.1. Dengan hasil ini, dapat disimpulkan bahwa VLAN30 juga telah dikonfigurasi dengan benar.



Gambar 11. Pengujian Ether5

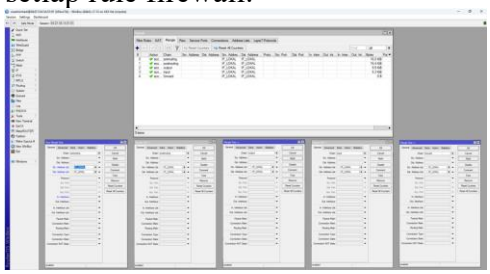
Hasil pengujian menunjukkan bahwa perangkat yang terhubung dengan Ether5 dapat mendapatkan alamat IP dari subnet yang dikonfigurasi untuk Ether5 sesuai dengan pengaturan yang ditetapkan pada perangkat jaringan.



Gambar 12. Penambahan Address List pada Firewall

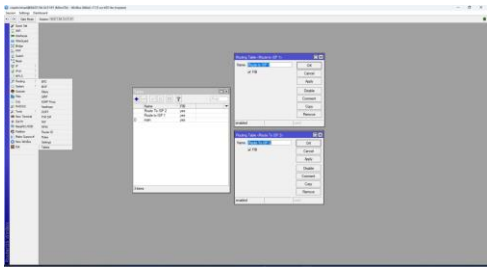
Address list dibuat di firewall Mikrotik untuk memudahkan pengelolaan akses pada firewall. Selain itu, address list juga digunakan untuk menyederhanakan proses manajemen trafik jaringan di firewall. Dalam konfigurasi ini, address list dibagi menjadi dua kategori utama, yaitu IP_LOKAL dan ISP. Untuk mempermudah penerapan aturan firewall yang berlaku untuk semua segmen jaringan lokal, alamat IP dari interface ether3, ether4, ether5, dan VLAN yang sudah dikonfigurasikan, yaitu VLAN1, VLAN2, dan VLAN3 dimasukkan ke dalam address list yang disebut IP_LOKAL. Dengan demikian, jika ada perubahan atau penambahan subnet di masa mendatang, cukup dengan menambahkan subnet IP baru ke dalam address list tersebut. Dalam hal ini, address list IP_LOKAL mengandung enam IP address, yaitu ether3, ether4, ether5, VLAN1, VLAN2, dan VLAN3.

Address list ISP2 hanya mencakup IP VLAN2 karena VLAN2 diarahkan melalui ISP2 untuk memisahkan jalur trafik keluar dari segmen jaringan departemen security yang menggunakan VLAN2. VLAN1 dan VLAN3 diarahkan ke ISP1. Dengan adanya address list, banyak IP atau range IP yang dapat dikelompokkan berdasarkan interface atau VLAN. Hal ini mempermudah membuat aturan firewall yang berlaku untuk banyak IP atau interface sekaligus, tanpa perlu menambah alamat IP satu per satu ke dalam setiap rule firewall.



Gambar 13. Konfigurasi Firewall Mangle untuk Trafik Internal (IP_LOKAL)

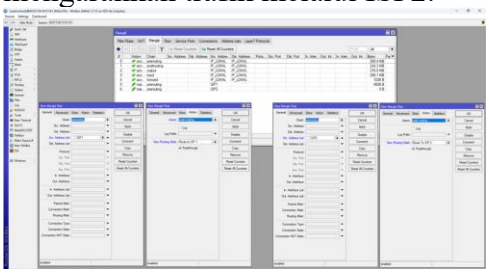
Aturan mangle dibuat untuk mengatur trafik internal di jaringan lokal. Address list IP_LOKAL digunakan untuk mengelompokkan semua alamat IP dari Ether dan VLAN yang telah dikonfigurasi sebelumnya. Firewall mangle menggunakan lima aturan utama untuk setiap chain dasar, yaitu prerouting, postrouting, output, input, dan forward. Aturan ini menggunakan IP_LOKAL sebagai src address list dan dst address list.



Gambar 14. Konfigurasi Routing Table

Setelah menyelesaikan konfigurasi dasar untuk mengelola trafik internal, langkah selanjutnya adalah mengarahkan trafik ke ISP yang sesuai. Untuk melakukan ini, konsep mark routing digunakan untuk menandai paket trafik yang akan diarahkan ke masing-masing ISP. Rute khusus untuk ISP dibuat dengan menggunakan tabel routing. Dua rute

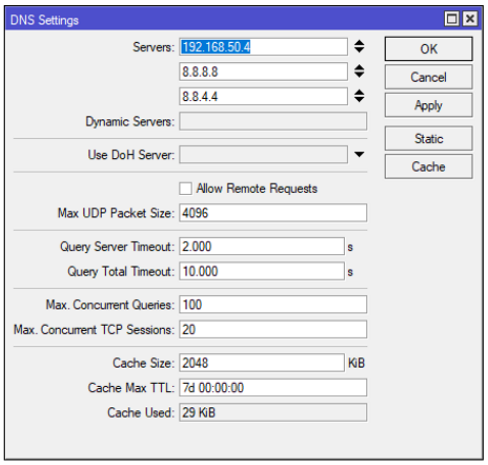
utama dibuat, yaitu “Route to ISP 1” untuk mengarahkan trafik melalui ISP1 dan “Route to ISP 2” untuk mengarahkan trafik melalui ISP2.



Gambar 15. Konfigurasi Mark Routing

Langkah selanjutnya adalah kembali ke firewall mangle untuk melakukan marking traffic yang akan diarahkan ke masing-masing ISP. Pada tahap ini, dua aturan tambahan didaftarkan ke dalam mangle. Prerouting untuk ISP menggunakan src address list yang berisi ISP1. Trafik dari VLAN1 dan VLAN3 yang sudah dimasukkan ke address list ISP1 akan ditandai dengan mark routing "Route to ISP 1", memastikan bahwa paket-paket dari VLAN1 dan VLAN3 akan diarahkan ke ISP1. Action yang digunakan adalah mark routing dan new routing mark diset ke "Route to ISP 1". Prerouting untuk ISP2 menggunakan src address list yang berisi ISP2. Action yang digunakan adalah mark routing dengan new routing mark diset ke "Route to ISP 2".

Setelah menandai trafik dalam mangle, langkah berikutnya adalah memastikan tabel routing dikonfigurasi dengan benar untuk mengarahkan lalu lintas ke gateway masing-masing ISP. Pada Route List untuk ISP1, IP ether1 ditambahkan sebagai gateway untuk routing table "main" dan "Route to ISP 1", yang berarti bahwa semua trafik yang ditandai dengan "Route to ISP 1" akan keluar melalui ether1 yang terhubung ke ISP1. Pada Route List untuk ISP2, IP ether2 ditambahkan sebagai gateway untuk routing table "main" dan "Route to ISP 2". Dengan pengaturan ini, trafik yang ditandai dengan "Route to ISP 2" akan diarahkan keluar melalui ether2 yang terhubung ke ISP2. Dengan demikian, trafik dari VLAN1 dan VLAN3 akan diarahkan ke ISP1 melalui ether1, sedangkan trafik dari VLAN2 akan diarahkan ke ISP2 melalui ether2, sesuai dengan marking yang dibuat di mangle. Selain itu, routing table "main" juga mengarahkan trafik melalui ether1 dan ether2 untuk trafik internet yang tidak secara khusus ditandai.



Gambar 16. Konfigurasi DNS

DNS (Domain Name System) server dikonfigurasi untuk memastikan bahwa perangkat dalam jaringan dapat mengakses nama domain dengan cepat dan akurat. DNS dari gateway lokal dikombinasikan dengan DNS publik Google (8.8.8.8 dan 8.8.4.4). Dengan konfigurasi ini, perangkat di jaringan lokal dapat mengakses situs web di internet tanpa kendala yang berkaitan dengan nama domain.

Setelah konfigurasi jaringan pada perangkat MikroTik selesai,

pengujian kecepatan internet dilakukan pada tiga VLAN yang telah dibuat. Tujuannya adalah untuk memastikan bahwa routing berjalan sesuai dengan konfigurasi yang telah dibuat, termasuk penerapan routing mark pada firewall mangle untuk memisahkan trafik berdasarkan sumber dan tujuan VLAN yang terhubung ke ISP yang berbeda. Pengujian dilakukan dengan menyambungkan kabel LAN yang terhubung ke komputer ke port switch layer 3. Setiap VLAN diuji secara terpisah untuk memastikan apakah routing ke internet melewati jalur ISP yang tepat. Kecepatan download dan upload pada setiap VLAN diukur dengan Speedtest, alat pengukur kecepatan internet.

Gambar 17. Pengujian Kecepatan Internet VLAN1

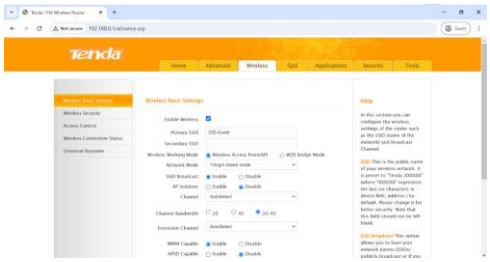
Hasil dari pengujian menunjukkan bahwa VLAN1 (VLAN10) dirouting melalui ISP1 yang terhubung dengan Ether1. Hasil kecepatan untuk mengunduh menunjukkan routing berhasil karena jalur trafik melalui ISP1. Kecepatan untuk mengunggah juga sesuai dengan kecepatan layanan yang diberikan oleh ISP1. Proses routing VLAN1 berjalan sesuai dengan konfigurasi yang telah ditentukan.

Gambar 18. Pengujian Kecepatan Internet VLAN2

Hasil pengujian kecepatan menunjukkan bahwa ISP2 terhubung dengan baik, sesuai dengan rute yang ditentukan oleh firewall mangle. Kecepatan unggah sesuai dengan ketentuan dari ISP2. Routing VLAN2 berjalan dengan baik dan trafik diarahkan melalui ether2 (ISP2) sesuai dengan pengaturan yang telah dibuat.

Gambar 19. Pengujian Kecepatan Internet VLAN3

Hasil pengujian menunjukkan bahwa trafik dikirim melalui ISP1, sesuai dengan konfigurasi firewall mangle. Kecepatan unggahan juga sesuai dengan layanan yang disediakan oleh ISP1. Routing untuk VLAN3 juga berjalan sesuai dengan pengaturan. Berdasarkan hasil pengujian, konfigurasi jaringan telah diimplementasikan dengan baik. Setiap VLAN memiliki kecepatan internet yang menandakan bahwa masing-masing VLAN menggunakan jalur ISP yang sesuai dengan pengaturan mark routing pada firewall mangle.

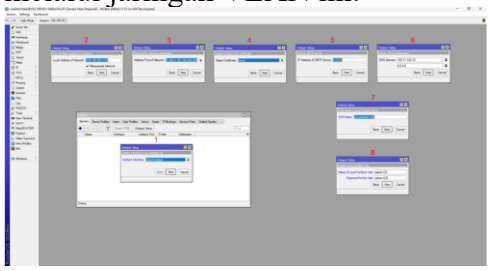


Gambar 20. Konfigurasi Wireless Router untuk Hotspot

Hotspot dibuat agar tamu yang mengunjungi perusahaan dapat dengan mudah mengakses internet. Setelah wireless router di reset, router diakses melalui browser dengan alamat IP defaultnya. Untuk membuat jaringan khusus untuk tamu, di halaman konfigurasi SSID diatur menjadi "CIS-Guest".

Gambar 21. Pembuatan VLAN untuk Hotspot

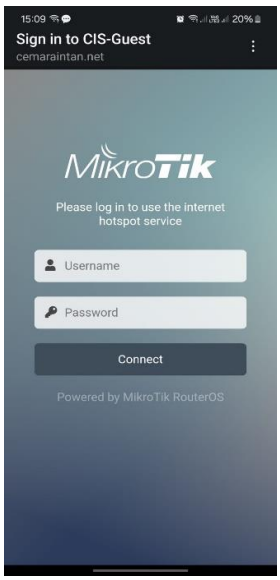
Selanjutnya, VLAN4 ditambahkan ke interface ether5 pada router. Setelah VLAN4 ditambahkan, langkah berikutnya adalah memberikan alamat IP untuk VLAN tersebut. Ini memastikan bahwa perangkat yang terhubung akan mendapatkan alamat IP yang tepat dan dapat berkomunikasi dengan baik melalui jaringan VLAN ini.



Gambar 22. Hotspot Setup

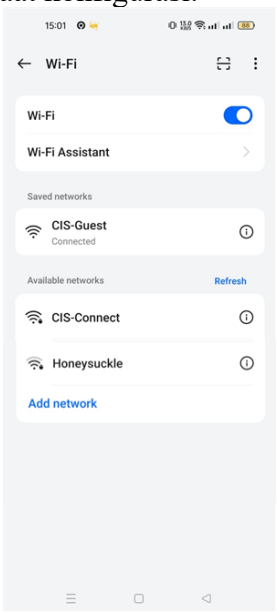
Konfigurasi hotspot pada VLAN4 dimulai dengan memilih interface hotspot VLAN4. Kemudian, alamat lokal jaringan VLAN4 diatur. Selanjutnya, pool IP ditambahkan ke jaringan, yang menentukan rentang alamat IP yang akan diberikan kepada perangkat yang terhubung. Nama DNS server dan nama DNS yang akan digunakan dalam jaringan juga diatur. Selain itu, nama pengguna dan kata sandi untuk hotspot lokal juga ditentukan.

Setelah menyelesaikan konfigurasi dasar hotspot, lima pengguna baru ditambahkan ke bagian pengguna hotspot dengan nama user1 hingga user5. Setiap pengguna hotspot ini diberikan batasan jumlah byte input/output sebesar 10 MB. Ini membatasi jumlah data yang dapat mereka unduh dan unggah melalui jaringan hotspot. Pembatasan ini diterapkan untuk menjaga kinerja jaringan stabil dan mencegah penggunaan bandwidth yang berlebihan.



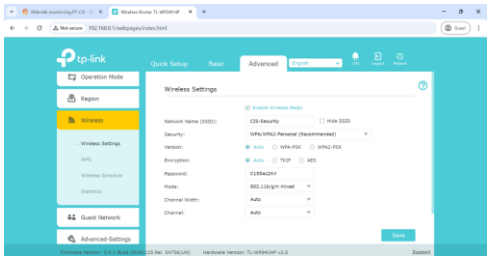
Gambar 23. Tampilan Saat Ingin Connect ke Hotspot

Setelah konfigurasi hotspot VLAN4 selesai, perangkat seluler dihubungkan ke jaringan hotspot dengan menggunakan SSID yang telah ditetapkan sebelumnya. Pengguna akan diarahkan secara otomatis ke halaman login ketika mereka memilih jaringan WiFi "CIS-Guest". Pengguna mengakses halaman melalui DNS name yang telah dikonfigurasi sebelumnya dan diminta untuk memasukkan nama pengguna dan kata sandi yang telah dibuat saat konfigurasi.



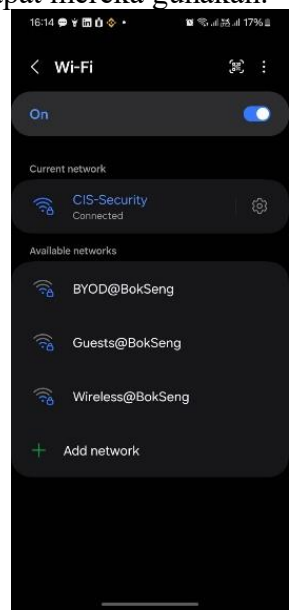
Gambar 24. Tampilan Setelah Terhubung ke Hotspot

Pengujian ini memastikan proses pengalihan ke halaman login berjalan dengan baik, sehingga pengguna dapat melakukan autentikasi sebelum dapat mengakses internet. Selain itu, proses ini memastikan bahwa jaringan hotspot beroperasi dengan baik, sehingga pengguna dapat mengaksesnya dengan aman tanpa mengganggu jaringan internal perusahaan.



Gambar 25. Konfigurasi Wireless Router untuk Security

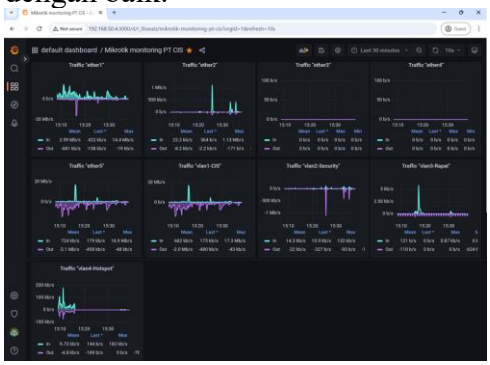
Setelah konfigurasi hotspot selesai, wireless router kedua direset. Router kedua ini dibuat untuk departemen security dan hanya dapat digunakan oleh staf yang memiliki akses. Setelah router direset, akses dapat dilakukan melalui browser dengan alamat IP default, dan SSID diubah menjadi "CIS-Security". Kata sandi juga diatur untuk memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses jaringan ini. Selanjutnya, wireless router ditempatkan di area security agar dapat mereka gunakan.



Gambar 26. Tampilan Setelah Terhubung ke WiFi Security

Setelah pemasangan WiFi selesai, pengujian konektivitas dilakukan dengan menghubungkan

perangkat seluler ke jaringan WiFi dengan menggunakan SSID yang telah diatur, yaitu "CIS-Security". Untuk mengakses jaringan ini, pengguna diminta untuk memasukkan kata sandi yang telah ditetapkan sebelumnya. Tujuan dari pengujian ini adalah untuk memastikan bahwa koneksi berjalan dengan baik.



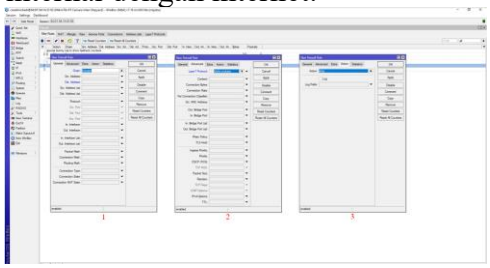
Gambar 27. Monitoring Jaringan di Grafana

Pada tahap operasional, pemantauan jaringan dilakukan menggunakan Grafana untuk memberikan visualisasi data secara real-time dan historis. Monitoring trafik jaringan dilakukan dengan memanfaatkan panel Grafana yang mengumpulkan data dari router. Tujuan dari monitoring trafik jaringan adalah untuk memantau jumlah bandwidth yang digunakan oleh setiap port perangkat jaringan untuk memastikan bahwa kapasitas jaringan tidak melebihi ambang batas dan mengidentifikasi pola trafik yang tidak biasa seperti lonjakan mendadak atau serangan siber. Dengan data historis, pengoptimalan atau pengembangan jaringan dapat direncanakan sesuai dengan kebutuhan bisnis. Hasil monitoring menunjukkan trafik jaringan yang konsisten yang sesuai dengan beban kerja perusahaan. Tidak ditemukan anomali pada trafik jaringan selama proses monitoring. Jika terjadi gangguan, Grafana akan memberikan indikasi visual dalam bentuk peringatan yang memungkinkan penanganan cepat.

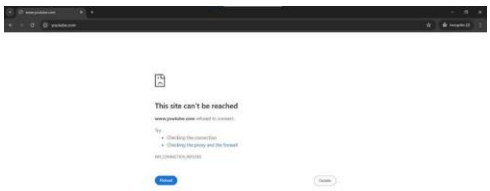
Sebagai bagian dari upaya peningkatan berkelanjutan keamanan jaringan, penambahan firewall rules dasar dilakukan untuk memblokir akses ke situs-situs tertentu yang dapat mengganggu produktivitas, membuka potensi kebocoran data, atau mengandung konten yang melanggar kebijakan perusahaan. Hal ini dilakukan untuk menjaga keamanan jaringan dan memastikan penggunaan internet yang sesuai dengan kebutuhan operasional perusahaan.

Gambar 28. Penambahan Firewall L7 Protocol

Konfigurasi dilakukan dengan membuat firewall rules berbasis Layer 7 Protocol pada perangkat MikroTik. Situs yang ingin diblokir dimasukkan sebagai parameter dalam rule dan diterapkan pada interface yang menghubungkan jaringan internal dengan internet.



Gambar 29. Penambahan Filter Rules



Gambar 30. Hasil Blokir Situs

Selain membatasi akses, langkah ini merupakan bagian dari penguatan sistem keamanan jaringan untuk mengurangi ancaman eksternal. Aturan firewall ini diharapkan membuat jaringan internal lebih aman, stabil, dan digunakan secara optimal untuk kepentingan operasional perusahaan.

Setelah perancangan dan implementasi jaringan baru, evaluasi dilakukan untuk menilai manfaat yang diperoleh perusahaan. Berdasarkan wawancara yang dilakukan dengan admin di PT Cemara Intan Shipyard, kondisi stabilitas dan performa jaringan saat ini telah meningkat jika dibandingkan dengan sebelumnya, yaitu koneksi internet menjadi jauh lebih stabil. Mereka menyampaikan bahwa, berbeda dengan kondisi yang sering mengalami masalah koneksi yang tidak stabil, saat ini mereka menikmati pengalaman penggunaan internet yang lebih konsisten dan lancar.

Penanganan masalah jaringan juga menjadi lebih efektif berkat penerapan kerangka kerja PPDIOO. Hal ini secara langsung memengaruhi kualitas layanan yang dirasakan dalam melaksanakan tugas sehari-hari. Secara keseluruhan, pelaksanaan kegiatan ini telah membantu perusahaan dalam menjaga kualitas layanan jaringan komputer agar tetap optimal, sehingga meningkatkan produktivitas dan memastikan kelancaran operasional bisnis bagi seluruh pengguna. Hal ini secara langsung mendukung tujuan perusahaan dalam menyediakan layanan yang andal dan efisien.

Simpulan

Pelaksanaan kegiatan yang berfokus pada perancangan dan implementasi jaringan perusahaan telah berhasil memenuhi tujuan utama yang telah ditentukan. Masalah kestabilan internet yang sebelumnya sering mengalami fluktuasi hingga Request Time Out (RTO), kini telah berhasil diatasi dengan baik. Dengan penerapan metode PPDIOO, penambahan core router, penerapan VLAN untuk segmentasi jaringan, serta pengaturan rute trafik yang tepat, konektivitas internet perusahaan kini lebih stabil, andal, dan aman. Jaringan yang telah diimplementasi memungkinkan optimasi penggunaan bandwidth dari ISP, yang secara langsung mendukung peningkatan produktivitas dan kelancaran operasional bisnis.

Rekomendasi untuk penelitian selanjutnya dapat berfokus pada pengembangan dan penerapan solusi failover internet yang lebih andal secara otomatis dengan memanfaatkan koneksi dari penyedia layanan internet (ISP) yang berbeda. Langkah ini penting untuk menciptakan redundansi infrastruktur yang nyata dan mengurangi risiko downtime akibat hanya mengandalkan satu provider.

Dengan penuh rasa hormat, penulis menyampaikan rasa terima kasih yang sebesar-besarnya kepada

semua pihak yang telah memberikan dukungan, bimbingan, dan fasilitas selama pelaksanaan kegiatan ini. Ucapan terima kasih ditujukan kepada Universitas Internasional Batam, khususnya Program Studi Teknologi Informasi, Bapak Haeruddin, S.Kom., M.MSI. dan Bapak Gautama Wijaya, S.Kom., M.T.I. selaku dosen pembimbing. Ucapan terima kasih juga ditujukan kepada PT Cemara Intan Shipyard dan Bapak Hadi Kusuma Dinata selaku pembimbing lapangan, atas arahan dan pengetahuan yang diberikan sehingga proyek ini dapat terlaksana dengan baik dan memberikan manfaat bagi perusahaan. Tanpa adanya dukungan dari berbagai pihak ini, kegiatan tidak akan dapat diselesaikan dengan optimal.

Daftar Pustaka

Antoro, B. S. D. (2014). *Optimalisasi Jaringan Internet Menggunakan Mikrotik di SMP Negeri 5 Depok* [Universitas Islam Negeri Sunan Kalijaga]. https://informatika.uin-suka.ac.id/media/dokumen_akademik/65_20190708_KP Final.pdf

Br Sipayung, P. I. O., Purba, V., & Agussalim, A. (2024). Analisis, Perancangan, dan Simulasi Jaringan VLAN Menggunakan Metode PPDIOO (Studi Kasus: SMAS Santo Yusup Surabaya). *TeknoIS : Jurnal Ilmiah Teknologi Informasi Dan Sains*, *14*(1), 110–118. https://doi.org/10.36350/jbs.v14i1.237

Habibullah, M. A., Pasha, H., Husein, M. N., & Sulaksono, D. H. (2022). *Penerapan Metode Ppdioo Pada Jaringan Internet Berbasis WLAN SMA Negeri 11 Surabaya*. *1*(2), 656–667. https://doi.org/10.31284/p.semtik.2022-1.3182

Hamza, S. (2022). Pemanfaatan Firewall Mangle Untuk Pengaturan Packet Data Menggunakan Mark Connection Mark Packet dan Mark Rouring dengan RouterBoard RB941-2nD. *Jurnal BIOSAINSTEK*, *4*(2), 27–33. https://doi.org/10.52046/biosainstek.v4i2.1055

Octaviyana, R. A., & Soewito, B. (2023). Perancangan Ulang Topologi Jaringan Dengan Kerangka Kerja Ppdioo. *Teknologi*, *13*(1), 33–41. https://doi.org/10.26594/teknologi.v13i1.3852

PT Cemara Intan Shipyard. (n.d.). *PT Cemara Intan Shipyard*. https://www.cemaraintan.com

Ramadhan, A. D., Negara, R. M., Azzahra, R. W., Rahmadi, B., & Radianto, D. O. (2024). Peran Teknologi Informasi dalam Transformasi di Industri Perkapalan. *Globe: Publikasi Ilmu Teknik, Teknologi Kebumian, Ilmu Perkapalan*, *2*(2), 30–51. https://doi.org/10.61132/globe.v2i2.253

Ramadhani, A., Palasara, N., & Gani, A. (2025). Filtering Firewall dan Manajemen Bandwidth untuk Keamanan Jaringan pada Kelurahan Buaran Indah. *Remik: Riset Dan E-Jurnal Manajemen Informatika Komputer*, *9*(1), 346–355. https://doi.org/http://doi.org/10.

33395/remik.v9i1.14482

Sangi, A. B., Sangkop, F. I., & Kembuan, O. (2023). Perancangan Dan Implementasi Jaringan Internet Berbasis Mikrotik. *Jurnal Penelitian Rumpun Ilmu Teknik*, *2*(2), 170–186. https://doi.org/10.55606/juprit.v2i2.1938

Ufia, S., Nugroho, A. D., & Wahjoedi, T. (2024). Meningkatkan Kompetensi Mahasiswa melalui Program Magang Sebagai Upaya Peningkatan Hard Skill dan Soft Skill. *Journal of Knowledge and Collaboration*, *1*(2), 39–47. https://doi.org/10.59613/97dmmj73

Umah, N. T., Yudanto, F. A., & Rilvani, E. (2025). Evaluasi Segmentasi VLAN dalam Optimalisasi Kinerja dan Keamanan pada Jaringan LAN di Universitas Pelita Bangsa. *Jurnal Ilmiah ILKOMINFO - Ilmu Komputer & Informatika*, *8*(1), 38–47. https://doi.org/10.47324/ilkominfo.v8i1.313

Wijoyo, A., Ichsani, D., Chotimah, I. N., Affia, N. P., & Anggana, N. (2023). Pengaruh Sistem Informasi Terhadap Efisiensi Operasional Perusahaan. *TEKNOBIS: Jurnal Teknologi, Bisnis, Dan Pendidikan*, *1*(2), 1–8. https://jurnalmahasiswa.com/index.php/teknobis/article/view/443

Yuliana, D., & Mogi, I. K. A. (2020). Computer Network Design Using PPDIOO Method With Case Study of SMA Negeri 1 Kunir. *JELIKU (Jurnal Elektronik Ilmu Komputer Udayana)*, *9*(2), 235. https://doi.org/10.24843/JLK.2020.v09.i02.p10