

BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Penelitian terdahulu merupakan referensi penting dalam menyusun dan mengembangkan penelitian ini. Bagian ini berfungsi untuk meninjau berbagai hasil penelitian sebelumnya yang berkaitan dengan implementasi infrastruktur jaringan, khususnya pada penggunaan perangkat MikroTik dan pengelolaan VLAN. Penelitian-penelitian terdahulu memberikan landasan teori, metode praktis, dan bukti empiris yang dapat digunakan untuk memperkuat argumen serta mendukung pelaksanaan penelitian ini. Dengan mengacu pada hasil penelitian sebelumnya, diharapkan penelitian ini dapat memberikan kontribusi baru yang relevan dan signifikan terhadap bidang ini. Berikut adalah tiga penelitian terdahulu yang relevan dengan implementasi infrastruktur jaringan pada perusahaan travel agent. Berikut adalah tiga penelitian terdahulu yang relevan dengan implementasi infrastruktur jaringan pada perusahaan travel agent.

Dalam penelitian ini, beberapa penelitian terdahulu digunakan sebagai landasan dan acuan dalam perancangan dan Implementasi Infrastruktur Jaringan Pada Perusahaan Travel Agent. Oleh sebab itu sebelum memulai penelitian perlu dilakukan eksplorasi dan studi pustaka baik melalui internet maupun jurnal – jurnal yang relevan dengan topik Implementasi Infrastruktur Jaringan Pada Perusahaan Travel Agent. Berikut adalah beberapa penelitian yang dijadikan tinjauan pustaka. Pada beberapa halaman selanjutnya disediakan table perbandingan antar-penelitian yang dapat dilihat pada Tabel 2.1.

Penelitian pertama dilakukan oleh **Wandi Syahindra (2022)** dengan judul *“Perancangan dan Implementasi Router Mikrotik pada Infrastruktur Jaringan Komputer Internet dengan Media Transmisi Wired dan Nirkabel (Studi Kasus IAIN Curup)”* dengan latar belakang penelitian ini dilakukan karena jaringan komputer di IAIN Curup sering mengalami permasalahan seperti pembagian bandwidth yang

tidak merata antar gedung, konflik IP address, dan kurangnya manajemen jaringan untuk mengoptimalkan penggunaan sumber daya. Tujuan penelitian bertujuan untuk merancang dan mengimplementasikan router MikroTik untuk mengatasi masalah pembagian bandwidth, meningkatkan efisiensi alokasi IP address, dan mengintegrasikan media transmisi kabel dan nirkabel pada jaringan komputer. Dengan metode penelitian dilakukan dengan pendekatan studi kasus, yang melibatkan Analisis kebutuhan jaringan dengan Mengidentifikasi jumlah perangkat, kebutuhan bandwidth, dan struktur jaringan. Konfigurasi MikroTik dengan mengatur routing, pembagian bandwidth menggunakan teknik queue tree, dan pengelolaan DHCP untuk menghindari konflik IP. Dan melakukan pengujian Mengukur performa jaringan setelah implementasi untuk memastikan hasil yang optimal.

Penelitian kedua dilakukan oleh **Fatkhurrahman dan Arita Witanti (2024)** dengan judul “*Optimasi Segmentasi Jaringan melalui Implementasi VLAN Dinamis pada Infrastruktur Kabel dan Nirkabel dengan MikroTik*” dengan latar belakang penelitian dilakukan untuk mengatasi tantangan dalam manajemen dan keamanan jaringan komputer yang kompleks dengan jumlah pengguna yang terus bertumbuh. Implementasi VLAN dinamis pada jaringan kabel dan nirkabel menggunakan MikroTik diharapkan dapat meningkatkan skalabilitas, fleksibilitas, dan keamanan jaringan. Tujuan penelitian ini bertujuan untuk mengoptimalkan segmentasi jaringan, meningkatkan keamanan, dan kinerja jaringan melalui penerapan VLAN dinamis pada infrastruktur kabel dan nirkabel dengan MikroTik. Menggunakan metode Analisis kebutuhan jaringan dengan Mengidentifikasi perangkat dan pengguna yang memerlukan segmentasi jaringan. Implementasi VLAN dinamis: Mengkonfigurasi VLAN dinamis pada perangkat MikroTik RouterOS untuk segmentasi jaringan yang efektif, dan pengujian serta evaluasi untuk mengukur kinerja jaringan sebelum dan sesudah implementasi VLAN dinamis untuk menilai peningkatan yang dicapai.

Penelitian ketiga dilakukan oleh **Luth Fian Alghifari, Dedi Irawan, dan Sudarmaji (2024)** dengan judul “*LOGIN OTOMATIS MENGGUNAKAN MAC ADDRESS PADA RB750Gr3 UNTUK MENINGKATKAN KEAMANAN*

JARINGAN WIFI PKBM RONAA” dengan latar belakang penelitian Penelitian ini bertujuan untuk meningkatkan keamanan jaringan Wi-Fi di PKBM RONAA dengan menerapkan sistem login otomatis berbasis MAC address pada Router Board RB750 Gr3. Sistem ini memungkinkan perangkat yang telah terdaftar untuk mengakses jaringan tanpa autentikasi manual berulang, dengan mengasosiasikan setiap perangkat yang diizinkan dengan MAC address uniknya. Tujuan dilakukan penelitian ini untuk meningkatkan pengendalian akses jaringan Wi-Fi melalui sistem login otomatis berbasis MAC address, sehingga hanya perangkat yang diotorisasi dapat terhubung. Metode yang digunakan yaitu dengan analisis kebutuhan jaringan mengidentifikasi perangkat yang memerlukan autentikasi jaringan, konfigurasi Router MikroTik: Menerapkan sistem login otomatis berbasis MAC address, dan Pengujian dan evaluasi: Mengukur efektivitas pengendalian akses jaringan sebelum dan sesudah implementasi.

Penelitian keempat dilakukan oleh **Nanang Sadikin dan Ahmad Fatih (2020)** dengan judul “*Perancangan dan Implementasi Jaringan Hotspot Berbasis Mikrotik pada PT. Bank XYZ*” dengan latar belakang penelitian ini dilakukan untuk merancang dan mengimplementasikan jaringan hotspot yang aman dan efisien menggunakan Mikrotik pada PT. Bank XYZ. Hal ini bertujuan untuk mengoptimalkan konektivitas bagi karyawan dan nasabah. Penelitian bertujuan untuk meningkatkan efisiensi dan keamanan akses internet melalui implementasi jaringan hotspot berbasis Mikrotik. Menerapkan pengaturan hotspot termasuk manajemen bandwidth dan autentikasi pengguna, serta mengukur kinerja jaringan setelah implementasi untuk memastikan hasil yang optimal.

Penelitian kelima dilakukan oleh **Febriayandi (2022)** dengan judul “*Perancangan Sistem Keamanan Jaringan dengan Metode MAC Address Filtering dan Penerapan Fitur Hotspot di Mikrotik RB-941 hAP Lite*” yang membahas penerapan keamanan jaringan melalui metode MAC Address Filtering dan fitur hotspot pada router MikroTik RB-941 hAP Lite. Studi ini dilakukan di lingkungan kantor Konsultan Pajak Edi Kurniawan dengan tujuan untuk mencegah akses tidak sah terhadap jaringan internal. Dalam penelitian ini, MAC Address Filtering

diterapkan untuk membatasi perangkat yang dapat mengakses jaringan, sedangkan fitur hotspot digunakan untuk mengelola autentikasi pengguna yang terhubung. Hasil penelitian menunjukkan bahwa kombinasi kedua metode ini mampu meningkatkan keamanan jaringan serta mengurangi risiko serangan dari perangkat yang tidak diotorisasi.

Penelitian keenam dilakukan oleh **Slamet Widodo dkk. (2022)** ini membahas *Keamanan Data Pengguna pada Jaringan Wireless Menggunakan Two-Factor Authentication, Password, dan MAC Address Filtering*. Dalam penelitian ini, akses jaringan dikontrol secara ketat dengan tiga lapisan pengamanan, yaitu:

1. Password: Digunakan sebagai metode dasar autentikasi pengguna.
2. Two-Factor Authentication (2FA): Digunakan untuk menambah lapisan keamanan dengan mengonfirmasi identitas pengguna.
3. MAC Address Filtering: Hanya perangkat yang sudah terdaftar yang dapat mengakses jaringan.

Hasil penelitian menunjukkan bahwa sistem keamanan ini efektif dalam mencegah akses ilegal dan meningkatkan stabilitas jaringan dengan mengurangi jumlah perangkat yang tidak dikenal yang mencoba terhubung ke jaringan.

PRO PATRIA

Penelitian ketujuh dilakukan oleh **Doni, M. Ulfa, dan H. D. Sabdho (2021)** yang meneliti *Implementasi Keamanan Jaringan Menggunakan Metode Port Blocking dan Port Knocking pada Mikrotik RB-941*. Metode Port Blocking digunakan untuk membatasi akses ke port tertentu guna mencegah eksloitasi oleh pengguna yang tidak sah. Sementara itu, metode Port Knocking diterapkan untuk memungkinkan akses hanya bagi pengguna yang mengetahui urutan port tertentu yang harus diakses sebelum mendapatkan izin koneksi. Hasil penelitian menunjukkan bahwa kombinasi Port Blocking dan Port Knocking mampu meningkatkan keamanan jaringan dengan cara menyembunyikan port yang tidak digunakan dan memberikan akses selektif hanya kepada perangkat yang diotorisasi. Teknik ini sangat efektif dalam mengurangi risiko serangan berbasis jaringan, seperti brute force attack dan scanning port.

Tabel 2.1 Penilitian Terdahulu

No	Peneliti	Judul Penelitian	Perumusan Masalah	Hasil
1.	Wandi Syahindra (2022)	Perancangan dan Implementasi Router Mikrotik pada Infrastruktur Jaringan Komputer Internet dengan Media Transmisi Wired dan Nirkabel (Studi Kasus IAIN Curup).	Bagaimana meningkatkan efisiensi jaringan komputer di IAIN Curup dengan meminimalkan konflik IP address dan membagi bandwidth secara merata?	Pembagian bandwidth menjadi lebih merata, konflik IP address berkurang, dan performa jaringan meningkat signifikan.
2.	Fatkhuurrhman dan Arita Witanti (2024)	Optimasi Segmentasi Jaringan melalui Implementasi VLAN Dinamis pada Infrastruktur Kabel dan Nirkabel dengan MikroTik.	Bagaimana menerapkan VLAN dinamis untuk meningkatkan skalabilitas, fleksibilitas, dan keamanan jaringan di lingkungan dengan pengguna yang terus bertambah?	Implementasi VLAN dinamis berhasil meningkatkan skalabilitas, fleksibilitas, dan keamanan jaringan, serta mengurangi broadcast untuk efisiensi bandwidth.

3.	Luth Fian Alghifari, Dedi Irawan, dan Sudarmaji (2024)	Login Otomatis Menggunakan Mac Address Pada RB750GR3 Untuk Meningkatkan Keamanan Jaringan Wifi Pkbm Ronaa	Bagaimana meningkatkan keamanan jaringan Wi-Fi dengan membatasi akses hanya pada perangkat yang terdaftar menggunakan autentikasi berbasis MAC address?	Sistem login berbasis MAC address meningkatkan keamanan dengan mencegah akses tidak sah, mempercepat proses autentikasi, dan mengurangi insiden ilegal.
4.	Nanang Sadikin dan Ahmad Fatih (2020)	Perancangan dan Implementasi Jaringan Hotspot Berbasis Mikrotik pada PT. Bank XYZ	Bagaimana merancang dan mengimplementasikan jaringan hotspot berbasis Mikrotik yang aman dan efisien untuk meningkatkan kualitas akses internet bagi karyawan dan nasabah di PT. Bank XYZ, termasuk pengelolaan bandwidth dan autentikasi pengguna untuk memastikan kestabilan konektivitas jaringan?	Implementasi jaringan hotspot berbasis Mikrotik meningkatkan keamanan, efisiensi bandwidth, dan stabilitas koneksi internet.merata berkat penerapan manajemen bandwidth yang optimal.

5.	Febriayandi (2022)	Perancangan Sistem Keamanan Jaringan dengan Metode MAC Address Filtering dan Penerapan Fitur Hotspot di Mikrotik RB-941 hAP Lite	Bagaimana penerapan MAC Address Filtering dan fitur hotspot dapat meningkatkan keamanan jaringan di kantor Konsultan Pajak?	Kombinasi MAC Address Filtering dan hotspot berhasil meningkatkan keamanan dan mengurangi risiko akses tidak sah.
6.	Slamet Widodo dkk. (2022)	Keamanan Data Pengguna pada Jaringan Wireless Menggunakan Two-Factor Authentication, Password, dan MAC Address Filtering	Bagaimana kombinasi autentikasi dua faktor, password, dan MAC Address Filtering dapat mencegah akses ilegal ke jaringan wireless?	Sistem keamanan ini efektif dalam mencegah akses ilegal dan meningkatkan stabilitas jaringan.
7.	Doni, M. Ulfah, dan H. D. Sabdho (2021)	Implementasi Keamanan Jaringan Menggunakan Metode Port Blocking dan Port Knocking	Bagaimana kombinasi metode Port Blocking dan Port Knocking dapat meningkatkan keamanan jaringan?	Metode ini berhasil menyembunyikan port tidak digunakan dan memberikan akses selektif hanya pada

		pada Mikrotik RB-941		perangkat yang diotorisasi.
--	--	-------------------------	--	--------------------------------

Berdasarkan penelitian-penelitian terdahulu yang telah dipaparkan, terlihat bahwa Penggunaan Perangkat MikroTik Router dapat diandalkan untuk mengelola routing, pembagian bandwidth, dan pengelolaan IP address, sehingga menjadi pilihan tepat untuk implementasi jaringan di perusahaan travel agent. Segmentasi jaringan menggunakan VLAN meningkatkan efisiensi dan keamanan, terutama dalam lingkungan dengan banyak divisi atau lantai, dan penggunaan autentikasi berbasis MAC address pada jaringan Wi-Fi memberikan perlindungan tambahan untuk mencegah akses tidak sah, memastikan jaringan hanya diakses oleh perangkat yang diotorisasi.

2.2 Kajian Teoritis

2.2.1 Infrastruktur Jaringan

Infrastruktur jaringan adalah kumpulan perangkat keras dan perangkat lunak yang digunakan untuk mendukung komunikasi data di suatu organisasi. Infrastruktur ini mencakup router, switch, access point, firewall, dan media transmisi lainnya. Menurut Tanenbaum & Wetherall (2011), jaringan komputer terdiri dari komponen perangkat keras dan perangkat lunak yang memungkinkan perangkat untuk berkomunikasi satu sama lain secara efisien dan aman. Selain itu, Kurose & Ross (2017) menjelaskan bahwa desain jaringan modern harus mampu mendukung skalabilitas, keamanan, dan ketersediaan yang tinggi untuk memenuhi kebutuhan bisnis yang berkembang. Infrastruktur jaringan yang baik akan memastikan konektivitas yang stabil, efisien, dan aman di lingkungan kerja.

2.2.2 Topologi Jaringan Komputer

Topologi jaringan menggambarkan bagaimana perangkat dalam jaringan diatur secara fisik atau logis. Forouzan (2013) menyebutkan bahwa pemilihan topologi yang tepat berdampak signifikan terhadap kinerja dan skalabilitas jaringan. Stallings (2014) menambahkan bahwa topologi seperti star, mesh, dan hybrid sering digunakan dalam jaringan modern karena mampu mengoptimalkan distribusi data

dan mengurangi risiko single point of failure. Pemilihan topologi yang sesuai akan mempengaruhi efisiensi komunikasi data dan kemudahan dalam manajemen jaringan..

2.2.3 Mikrotik sebagai Solusi Manajemen Jaringan

Mikrotik adalah perangkat jaringan yang dikenal karena fleksibilitas dan kemampuannya dalam manajemen jaringan. Mikrotik menggunakan *RouterOS*, sistem operasi berbasis Linux yang memungkinkan berbagai fungsi seperti routing, firewall, VPN, hingga manajemen bandwidth. Menurut Mikrotik (2020), perangkat ini sangat cocok untuk digunakan pada organisasi dengan kebutuhan jaringan yang kompleks, seperti distribusi ISP dan segmentasi trafik. Mikrotik memberikan kontrol penuh terhadap pengaturan IP, routing, dan pengelolaan traffic.

2.2.4 Manajemen Bandwidth dengan Mikrotik

Manajemen bandwidth penting untuk memastikan bahwa alokasi bandwidth di jaringan dapat mengoptimalkan penggunaan sumber daya yang ada. Gunawan (2018) menyatakan bahwa penggunaan teknik Queue dalam MikroTik memungkinkan pembatasan bandwidth secara dinamis berdasarkan prioritas. Permadi (2019) menunjukkan bahwa implementasi manajemen bandwidth menggunakan MikroTik RouterBoard di lingkungan pendidikan berhasil meningkatkan kualitas layanan internet dengan membatasi penggunaan bandwidth berdasarkan kebutuhan pengguna. Dengan manajemen bandwidth yang efektif, performa jaringan dapat ditingkatkan, terutama untuk aplikasi-aplikasi yang membutuhkan prioritas tinggi seperti VoIP dan video conference.

2.2.5 Manajemen Bandwidth dengan Queue Tree

Manajemen bandwidth adalah proses pengalokasian bandwidth secara optimal agar setiap pengguna mendapatkan akses yang adil sesuai dengan kebutuhannya. Mikrotik menyediakan fitur Queue Tree yang memungkinkan administrator jaringan untuk menetapkan batasan bandwidth bagi pengguna atau kelompok pengguna tertentu, sehingga mencegah pemakaian berlebihan yang dapat mengganggu performa jaringan.

2.2.6 Autentikasi MAC Address

Autentikasi MAC address adalah metode yang digunakan untuk membatasi akses jaringan berdasarkan identitas perangkat yang dikenal. Setiawan (2021) menjelaskan bahwa autentikasi MAC address memberikan lapisan keamanan tambahan di jaringan Wi-Fi dengan memfilter perangkat yang tidak terdaftar. Sistem ini efektif dalam mengontrol perangkat yang dapat mengakses jaringan, sehingga membantu mencegah akses tidak sah. Autentikasi ini sering digunakan di lingkungan kantor untuk memastikan hanya perangkat yang telah terdaftar yang dapat terhubung ke jaringan internal.

2.2.7 Monitoring Jaringan

Monitoring jaringan adalah kegiatan yang bertujuan untuk mengawasi lalu lintas data dan performa jaringan. Bejtlich (2013) menyebutkan bahwa monitoring jaringan yang efektif melibatkan pengumpulan, analisis, dan pelaporan data untuk mendeteksi anomali dan merespons insiden secara real-time. Observium (2024) sebagai salah satu perangkat lunak monitoring jaringan menyediakan antarmuka berbasis web yang memudahkan pengelolaan dan pemantauan infrastruktur jaringan secara menyeluruh. Monitoring jaringan yang baik memungkinkan deteksi dini terhadap potensi gangguan dan memastikan ketersediaan layanan jaringan tetap optimal.

2.2.8 Wireless LAN (Wi-Fi)

Wi-Fi adalah teknologi jaringan yang memungkinkan perangkat untuk terhubung ke internet tanpa kabel. Gast (2013) mengungkapkan bahwa standar IEEE 802.11 mendefinisikan protokol untuk komunikasi nirkabel yang aman dan efisien. Pratama (2022) menambahkan bahwa implementasi Wi-Fi berbasis 802.11ac di lingkungan perkantoran mampu meningkatkan kecepatan hingga 1 Gbps, membuatnya ideal untuk mendukung kebutuhan bisnis modern. Pengelolaan jaringan Wi-Fi yang baik, termasuk segmentasi jaringan untuk Guest dan karyawan, sangat penting untuk menjaga keamanan dan performa jaringan.

2.2.9 Perangkat Keras Jaringan (Hardware)

Perangkat keras jaringan seperti router, switch, dan access point menjadi komponen kunci dalam infrastruktur jaringan. Anggriyani (2020) menyebutkan

bahwa perangkat keras ini berfungsi untuk memfasilitasi transmisi data antar perangkat, memastikan komunikasi yang andal dan aman.

2.2.10 Perangkat Lunak Jaringan (Software)

Perangkat lunak jaringan digunakan untuk mengelola konfigurasi, pemantauan, dan keamanan jaringan. Bratha (2022) menyatakan bahwa perangkat lunak jaringan berperan penting dalam mengoptimalkan kinerja, memantau ancaman keamanan, dan mengelola lingkungan jaringan yang kompleks. Comer (2018) juga menyoroti peran perangkat lunak dalam mendukung protokol komunikasi, manajemen IP, dan routing yang efisien. Dengan perangkat lunak yang tepat, administrator jaringan dapat dengan mudah mengelola dan memantau infrastruktur jaringan secara efektif..

