BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Perkembangan teknologi jaringan *wireless* mengalami kemajuan pesat seiring dengan transformasi digital global yang mendorong kebutuhan konektivitas yang cepat dan fleksibel. Teknologi *wireless* kini menjadi tulang punggung utama dalam menyediakan layanan komunikasi data yang andal di berbagai sektor, termasuk industri, logistik, dan kesehatan (Ananda et al., 2025). Pertumbuhan signifikan perangkat *Internet of Things* (IoT) memperluas penggunaan jaringan *wireless* secara masif, memungkinkan perangkat tersebut saling berkomunikasi secara *real-time* dan mendukung otomatisasi proses bisnis (Prasetia & Widiasari, 2025). Teknologi Wi-Fi generasi terbaru seperti Wi-Fi 6 (802.11ax) menawarkan kecepatan yang jauh lebih tinggi, kapasitas yang lebih besar, serta efisiensi spektrum yang meningkat dibandingkan generasi sebelumnya (Ananda et al., 2025). Selain itu, jaringan 5G yang kini mulai diimplementasikan di Indonesia memberikan kecepatan transfer data yang tinggi dan latensi rendah, sehingga mampu memenuhi tuntutan era digital yang menuntut produktivitas dan mobilitas tinggi (Rizky et al., 2024). Oleh karena itu, pengembangan dan pengelolaan infrastruktur jaringan *wireless* yang andal menjadi kebutuhan mutlak dalam menjamin kelancaran komunikasi data serta keamanan informasi, khususnya di lingkungan industri modern yang sangat bergantung pada efisiensi dan kecepatan akses informasi.

Wireless Local Area Network (WLAN) memiliki peran krusial dalam mendukung mobilitas dan fleksibilitas kerja di berbagai lingkungan profesional. WLAN berperan strategis dalam kantor modern dan industri logistik dengan memfasilitasi komunikasi internal, akses *cloud*, serta kolaborasi *real-time* antar karyawan dan sistem. Penelitian oleh Saputra & Geni (2024) menunjukkan bahwa implementasi WLAN pada sebuah toko bangunan berhasil meningkatkan distribusi *bandwidth* dan

kualitas layanan internet, yang berdampak positif terhadap efisiensi operasional dan kepuasan pengguna di lingkungan kerja. Selain itu, penelitian oleh Ramadhan & Annisa (2024) menegaskan bahwa WLAN mendukung integrasi perangkat *Internet of Things* (IoT) yang semakin meluas di sektor industri, sehingga mempercepat otomasi proses bisnis dan meningkatkan responsivitas perusahaan. Dalam konteks pemerintahan daerah, analisis jaringan WLAN pada Badan Pengelolaan Keuangan dan Aset Daerah Sumatera Selatan menyoroti pentingnya strategi penempatan *access point* untuk menjamin kualitas sinyal dan mendukung produktivitas kerja tanpa hambatan kabel fisik (Usman, 2023). Dengan demikian, WLAN tidak hanya menghemat biaya infrastruktur kabel, tetapi juga meningkatkan efisiensi dan kecepatan akses data secara *real-time* yang sangat dibutuhkan dalam lingkungan kerja modern.

Meskipun memiliki banyak keunggulan, penerapan WLAN tidak terlepas dari berbagai tantangan infrastruktur yang dapat menghambat kinerja jaringan secara keseluruhan. Salah satu kendala utama adalah jangkauan sinyal yang terbatas, terutama di area yang banyak penghalang fisik seperti dinding dan peralatan elektronik, yang dapat menyebabkan penurunan kualitas sinyal dan cakupan jaringan yang tidak merata. Selain itu, interferensi antar perangkat *wireless* maupun dari sumber eksternal sering menjadi masalah yang mengganggu kestabilan koneksi WLAN, terutama pada frekuensi 2.4 GHz yang rentan terhadap tumpang tindih sinyal (Hermawan & Rahmatia, 2024). Fenomena *oversubscription*, yaitu kondisi di mana jumlah pengguna melebihi kapasitas *access point*, juga sering terjadi di lingkungan dengan kepadatan pengguna tinggi, sehingga menurunkan kualitas layanan dan pengalaman pengguna (Usman, 2023).

Kompleksitas pengelolaan perangkat keras seperti *access point* dan *router* serta perangkat lunak sistem manajemen jaringan menjadi tantangan tersendiri bagi administrator jaringan. Pengelolaan ini memerlukan optimalisasi dan monitoring yang berkelanjutan agar

jaringan tetap stabil dan efisien di tengah aktivitas pengguna yang dinamis dan kebutuhan *bandwidth* yang terus meningkat (Usman, 2023). Oleh karena itu, strategi penempatan *access point* yang tepat, penggunaan kanal frekuensi yang optimal, dan penerapan sistem monitoring jaringan yang efektif menjadi sangat penting untuk mengatasi tantangan tersebut dan menjamin kualitas layanan WLAN.

Wireless Local Area Network (WLAN) merupakan teknologi yang rawan tehadap berbagai ancaman keamanan siber, seperti penyadapan data *(sniffing*), *malware, exploit* jaringan, dan akses ilegal dari pihak luar. Kerentanan ini disebabkan oleh sifat transmisi data secara nirkabel yang memungkinkan pihak tidak berwenang untuk mengakses jaringan jika tidak dilindungi sistem keamanan yang memadai (Adiguna & Widagdo, 2022). Penelitian oleh Astrida et al., (2022) menunjukkan bahwa masih terdapat banyak celah keamanan pada jaringan *wireless* termasuk kerentanan terhadap serangan seperti WPA2 *cracking*, *Denial of Service* (DoS), dan *password cracking* pada *router*.

Serangan *sniffing* memungkinkan penyerang mencuri data sensitif yang sedang ditransmisikan, sementara *malware* dan *exploit* jaringan dapat dimanfaatkan untuk mengambil alih perangkat atau seluruh sistem (Adiguna & Widagdo, 2022). Penelitian oleh Kurnia & Mandasari (2023) menunjukkan bahwa pembatasan akses menggunakan mekanisme seperti *Access Control List* (ACL) dan monitoring trafik secara berkala dapat secara signifikan menutup celah keamanan tersebut.

Untuk mengatasi tantangan tersebut, penting diterapkan sistem keamanan berlapis, seperti penggunaan enkripsi data (misalnya WPA3), autentikasi pengguna yang kuat, serta monitoring dan evaluasi trafik secara rutin (Kurnia & Mandasari, 2023). Implementasi *Intrusion Detection System* (IDS) juga terbukti efektif dalam mengatasi dan mencegah serangan siber sebelum menyebabkan kerusakan lebih lanjut (Jufri & Heryanto, 2021). Dengan demikian, kombinasi antara teknologi enkripsi, autentikasi, dan monitoring menjadi kunci utama

dalam menjaga keamanan jaringan *wireless* di era digital yang semakin kompleks.

PT. SINGA LAUTAN INDONESIA merupakan perusahaan yang bergerak di bidang jasa pelayaran dan transportasi laut, khususnya dalam pengangkutan hasil tambang. Perusahaan ini merupakan sebuah grup usaha yang berfokus pada sektor pertambangan dan logistik di Indonesia. Sebagai perusahaan yang mengandalkan teknologi informasi, PT. SINGA LAUTAN INDONESIA menggunakan jaringan *Wireless Local Area Network* (WLAN) untuk mendukung operasional sehari-hari, khususnya dalam komunikasi internal, pertukaran data, dan aktivitas sistem informasi internal yang menjadi tulang punggung layanan perusahaan.

Ketergantungan perusahaan terhadap jaringan WLAN sangat tinggi, mengingat kebutuhan akses data yang cepat dan *real-time* untuk koordinasi antar divisi, pengelolaan armada kapal, serta logistik. Berdasarkan pengamatan awal, terdapat beberapa tantangan yang mulai dirasakan dalam implementasi jaringan ini, seperti gangguan sinyal yang menghambat komunikasi, risiko keamanan jaringan yang berpotensi mengancam data perusahaan, serta keterbatasan kapasitas WLAN yang menyebabkan penurunan performa saat jumlah pengguna meningkat. Tantangan-tantangan ini menuntut PT. SINGA LAUTAN INDONESIA untuk melakukan evaluasi menyeluruh terhadap infrastruktur dan sistem keamanannya. Oleh karena itu, perlu dilakukan analisis infrastruktur dan keamanan jaringan WLAN guna memastikan operasional perusahaan tetap berjalan secara optimal, efisien, dan aman.

Jaringan *Wireless Local Area Network* (WLAN) saat ini menjadi tulang punggung utama komunikasi dan pertukaran data di berbagai perusahaan, termasuk PT. SINGA LAUTAN INDONESIA. Namun, seiring dengan meningkatnya kompleksitas penggunaan dan ancaman keamanan siber, evaluasi infrastruktur dan keamanan jaringan WLAN secara menyeluruh menjadi hal yang krusial. Evaluasi ini bertujuan

untuk mengidentifikasi potensi kelemahan sistem yang sedang berjalan, baik dari sisi teknis maupun proteksi data, karena kelalaian dalam penanganan dapat berdampak pada gangguan layanan, kebocoran informasi, hingga serangan siber yang merugikan. Jika kelemahan ini tidak segera diatasi, PT. SINGA LAUTAN INDONESIA berisiko mengalami gangguan operasional yang signifikan atau bahkan kerugian finansial akibat serangan siber.

Oleh karena itu, diperlukan evaluasi menyeluruh terhadap kapasitas jaringan, jangkauan sinyal, serta efektivitas sistem keamanan seperti enkripsi dan autentikasi. Melalui analisis berbasis data dan pendekatan sistematis, perusahaan dapat memperoleh rekomendasi yang tepat guna untuk meningkatkan keandalan, keamanan, dan ketahanan jaringan WLAN. Hasil penelitian ini diharapkan menjadi acuan dalam pengambilan keputusan strategis terkait pengembangan infrastruktur jaringan, sekaligus mendukung peningkatan produktivitas dan keamanan operasional perusahaan. Evaluasi ini juga bertujuan menilai sejauh mana sistem WLAN yang ada mampu memenuhi kebutuhan operasional dan tuntutan bisnis yang terus berkembang. Dengan pendekatan analitis berbasis data aktual, PT. SINGA LAUTAN INDONESIA diharapkan memperoleh solusi teknis dan praktis yang relevan untuk memperkuat performa dan manajemen infrastruktur *wireless*. Temuan penelitian ini dapat menjadi dasar dalam merumuskan strategi pengembangan jaringan yang adaptif dan efektif di lingkungan industri modern.

1.2. Maksud dan Tujuan

Penelitian ini dilakukan untuk mengevaluasi secara menyeluruh infrastuktur dan kemanan jaringan *Wireless Local Area Network* (WLAN) di PT. SINGA LAUTAN INDONESIA. Evaluasi ini bertujuan untuk mengidentifikasi kelemahan teknis, keterbatasan kapasitas jaringan, serta potensi risiko keamanan yang dapat mengganggu kinerja dan operasional perusahaan. Melalui pemahaman

yang mendalam terhadap kondisi jaringan saat ini, penelitian ini diharapkan dapat memberikan rekomendasi perbaikan dan stategi pengembangan jaringan WLAN yang lebih andal dan aman di lingkungan perusahaan.

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

1. Menganalisis infrastuktur jaringan *Wireless Local Area Network* (WLAN) di PT. SINGA LAUTAN INDONESIA.
2. Menganalisis keamanan jaringan *Wireless Local Area Network* (WLAN) di PT SINGA LAUTAN INDONESIA.
3. Merumuskan rekomendasi teknis dan praktis untuk peningkatan infrastuktur dan keamanan jaringan *Wireless Local Area Network* (WLAN) di PT SINGA LAUTAN INDONESIA.

1.3. Metode Penelitian

1.3.1. Metode Pengumpulan Data

Untuk mencapai tujuan penelitian, data dikumpulkan melalui beberapa metode sebagai berikut:

1. Observasi Langsung

   Melakukan pengamatan langsung terhadap infrastruktur jaringan WLAN di PT. SINGA LAUTAN INDONESIA guna memahami topologi, arsitektur, dan konfigurasi perangkat keras yang digunakan. Fokus observasi meliputi identifikasi perangkat jaringan seperti *Access Point*, *router*, dan *switch*, penempatan perangkat, serta kondisi fisik lingkungan yang mempengaruhi performa jaringan. Observasi juga mencakup interferensi antar kanal radio dan pengaruh lingkungan fisik terhadap sinyal. Pengukuran kualitas sinyal dilakukan menggunakan aplikasi survey *Wi-Fi* dan *Speedtest by Ookla* untuk mengidentifikasi area dengan sinyal lemah dan mengukur performa jaringan secara real-time.
2. Wawancara

Menggunakan metode wawancara semi-terstruktur dengan tim IT dan pengguna jaringan untuk memperoleh informasi mengenai pengalaman penggunaan jaringan, masalah teknis yang dihadapi, serta kebutuhan dan ekspektasi terhadap sistem WLAN. Pertanyaan juga mencakup aspek pengelolaan trafik, manajemen *bandwidth*, penerapan *Quality of Service* (QoS), dan strategi peningkatan performa serta keamanan jaringan (Usman, 2023).

3. Studi Dokumentasi

   Mengumpulkan dan menelaah dokumen internal terkait jaringan WLAN, seperti diagram jaringan, konfigurasi perangkat, kebijakan keamanan, dan laporan performa. Analisis ini berguna untuk memahami struktur formal jaringan serta menilai kesesuaian dengan teknologi dan kebijakan yang diterapkan (Adiguna & Widagdo, 2022).

4. Pengujian Jaringan

   Pengujian jaringan WLAN di PT. SINGA LAUTAN INDOENSIA dilakukan melalui pengukuran kualitas sinyal menggunakan aplikasi *survey Wi-Fi* dan *Speedtest by Ookla*, pengujian kecepatan transfer data (*download, upload, latency, jitter, packet loss*), analisis trafik menggunakan *NetFlow* dan *Wireshark*, serta monitoring *log* jaringan melalui *Unifi Controller*. Evaluasi aspek keamanan dilakukan melalui telaah kebijakan, pengelolaan akses, dan analisis log autentikasi.

1.3.2. Analisa Penelitian

Data yang telah dikumpulkan akan dianalisis dengan beberapa pendekatan sebagai berikut:

1. Analisis Deskriptif Kualitatif

   Data hasil observasi, wawancara, dan studi dokumentasi akan dianalisis secara deskriptif kualitatif untuk menggambarkan kondisi infrastruktur jaringan serta sistem keamanan WLAN. Hasil analisis ini disajikan dalam bentuk narasi yang menjelaskan konteks,

permasalahan, dan pola temuan di lapangan, mencakup aspek topologi, konfigurasi perangkat, kebijakan keamanan, dan prosedur operasional.

2. Analisis Kuantitatif

   Data teknis yang diperoleh dari pengujian jaringan, seperti throughput, kekuatan sinyal (*signal strength*), latensi, dan kapasitas trafik, akan dianalisis secara kuantitatif. Hasilnya disajikan dalam bentuk tabel, grafik, dan diagram untuk membandingkan performa jaringan dengan kebutuhan operasional yang relevan, khususnya dalam aspek infrastruktur dan kinerja jaringan (Ananda et al., 2025).

3. Analisis SWOT (*Strengths, Weaknesses, Opportunities, Threats*)

   Analisis ini digunakan untuk mengidentifikasi kekuatan dan kelemahan internal jaringan WLAN serta peluang dan ancaman eksternal yang memengaruhi performa dan keamanan jaringan. Hasil analisis SWOT akan membantu merumuskan strategi pengembangan dan penguatan jaringan yang tepat sasaran dan berkelanjutan.

1.4. Ruang Lingkup

Penelitian ini difokuskan pada evaluasi dan analisis infrastruktur serta keamanan jaringan *Wireless Local Area Network* (WLAN) yang digunakan di kantor pusat PT. SINGA LAUTAN INDONESIA. Cakupan penelitian ini dibatasi pada jaringan WLAN saja dan tidak mencakup jaringan LAN kabel maupun infrastruktur di lokasi lain seperti cabang perusahaan atau kapal. Adapun ruang lingkup penelitian ini mencakup tiga aspek utama, yaitu:

1. Analisis Infrastruktur Jaringan WLAN
   1) Evaluasi topologi jaringan WLAN yang digunakan, meliputi struktur fisik dan logis jaringan.
   2) Identifikasi dan inventarisasi perangkat keras dan perangkat lunak jaringan seperti *Access Point*, *router*, *switch*, dan sistem pengelolaan jaringan.

3) Pengukuran kualitas sinyal (*signal strength*) dan cakupan area (*coverage area*) untuk memastikan konektivitas optimal.
4) Evaluasi kinerja jaringan melalui pengujian kecepatan transfer data (*throughput*), latensi, dan analisis kapasitas trafik untuk mengidentifikasi *bottleneck*.
5) Analisis penerapan *Quality of Service* (QoS) untuk menjamin prioritas trafik dan kestabilan layanan pada aplikasi kritikal.

2. Keamanan Jaringan
   1) Evaluasi kebijakan keamanan jaringan yang diterapkan, termasuk tata kelola akses dan pengawasan jaringan.
   2) Analisis mekanisme autentikasi dan enkripsi yang digunakan, seperti protokol WPA2/WPA3 dan sistem autentikasi tambahan (misalnya RADIUS).
   3) Evaluasi aspek keamanan jaringan melalui monitoring *log*, analisis trafik, dan telaah kebijakan serta pengelolaan akses jaringan untuk mengidentifikasi potensi celah keamanan.
   4) Monitoring dan deteksi ancaman dengan analisis trafik dan *log* jaringan untuk mendeteksi aktivitas mencurigakan.
   5) Evaluasi sistem deteksi dan pencegahan ancaman serta perumusan rekomendasi penguatan keamanan jaringan.