

Penerapan Teknologi Ubiquiti dalam Optimalisasi Jaringan Kantor Skala Menengah

Arib Nawwar Tahir^{1*}, Shafwan Abiyu Wirawan², Yuma Akbar³

¹ STIKOM Cipta Karya Informatika; email : aribtahir27@gmail.com

² STIKOM Cipta Karya Informatika; email : shafwanaw@gmail.com

³ STIKOM Cipta Karya Informatika; email : yuma.pji@gmail.com

* Arib Nawwar Tahir

Abstract: PT. ABC, a mining company in Southeast Sulawesi, faces serious problems in its network infrastructure, including connection instability, uneven bandwidth distribution, security vulnerabilities, and inefficient manual monitoring. This research implements a centralized network solution based on Ubiquiti UniFi Controller, supported by Cisco devices (ISR4321/K9 routers and WS-C3750V2 switches) and U6-Pro access points, to improve stability, security, and operational efficiency. Through a phased approach—analysis of existing networks, installations, VLAN and QoS configurations, and performance tests—the results showed significant improvements: downtime decreased by 83% (from 12 hours to 2 hours/month), throughput increased by 143% (35 Mbps to 85 Mbps), and critical application latency reduced by 77% (142 ms to 32 ms). Implementing security policies such as VLAN segmentation and firewalls successfully eliminates cyberattacks, while QoS ensures optimal bandwidth allocation for priority applications. The business impact includes savings of IDR 40 million/month, acceleration of the reporting process, and increased user satisfaction. This solution not only addresses technical issues but also provides a scalable and sustainable framework for similar companies in the mining and MSME sectors.

Keywords: Network; Security; Efficiency; Bandwidth; Monitoring.

Abstrak: PT. ABC, perusahaan pertambangan di Sulawesi Tenggara, menghadapi masalah serius dalam infrastruktur jaringannya, termasuk ketidakstabilan koneksi, distribusi bandwidth tidak merata, kerentanan keamanan, dan pemantauan manual yang tidak efisien. Penelitian ini mengimplementasikan solusi jaringan terpusat berbasis Ubiquiti UniFi Controller, didukung perangkat Cisco (router ISR4321/K9 dan switch WS-C3750V2) serta akses point U6-Pro, untuk meningkatkan stabilitas, keamanan, dan efisiensi operasional. Melalui pendekatan bertahap—analisis jaringan eksisting, instalasi, konfigurasi VLAN dan QoS, serta uji kinerja—hasilnya menunjukkan perbaikan signifikan: downtime turun 83% (dari 12 jam menjadi 2 jam/bulan), throughput meningkat 143% (35 Mbps ke 85 Mbps), dan latency aplikasi kritis berkurang 77% (142 ms ke 32 ms). Penerapan kebijakan keamanan seperti segmentasi VLAN dan firewall berhasil menghilangkan serangan siber, sementara QoS memastikan alokasi bandwidth optimal untuk aplikasi prioritas. Dampak bisnis mencakup penghematan Rp40 juta/bulan, percepatan proses pelaporan, dan peningkatan kepuasan pengguna. Solusi ini tidak hanya mengatasi masalah teknis tetapi juga menyediakan kerangka kerja yang skalabel dan berkelanjutan untuk perusahaan sejenis di sektor pertambangan dan UMKM.

Kata kunci: Jaringan Keamanan; Efisiensi; Bandwidth; Monitoring.

Diterima: Mei 05, 2025

Direvisi: Mei 19, 2025

Diterima: Juni 02, 2025

Diterbitkan: Juni 04, 2025

Versi sekarang: Juni 05, 2025



Hak cipta: © 2025 oleh penulis.

Diserahkan untuk kemungkinan

publikasi akses terbuka

berdasarkan syarat dan ketentuan

lisensi Creative Commons

Attribution (CC BY SA) (

1. Pendahuluan

Di tengah kemajuan era digital, kebutuhan perusahaan akan infrastruktur jaringan yang stabil dan andal menjadi semakin penting. PT. ABC, yang beroperasi di sektor pertambangan di Sulawesi Tenggara, menghadapi tantangan serius akibat ketidakstabilan jaringan. Masalah seperti distribusi bandwidth yang tidak merata, seringnya gangguan koneksi, serta sistem

<https://creativecommons.org/licenses/by-sa/4.0/>

manajemen jaringan yang tersebar menjadi hambatan utama dalam meningkatkan efisiensi dan produktivitas operasional [1]. Kondisi ini diperparah oleh meningkatnya risiko serangan siber, yang dapat mengancam keberlangsungan bisnis jika tidak segera ditangani secara strategis.

Sebagai solusi, penggunaan perangkat jaringan dari Ubiquiti, khususnya melalui platform UniFi Controller, diusulkan untuk mengintegrasikan dan memusatkan pengelolaan jaringan. Pendekatan ini memungkinkan pengawasan dan pengaturan jaringan secara menyeluruh, yang terbukti dapat meningkatkan stabilitas dan efisiensi operasional [2]. Penelitian menunjukkan bahwa pengelolaan bandwidth yang optimal melalui sistem terpusat dapat memperbaiki performa jaringan secara signifikan [3].

Selain itu, aspek keamanan jaringan menjadi prioritas utama. Dengan menerapkan segmentasi VLAN dan firewall filtering, perusahaan dapat membatasi akses tidak sah dan memperkuat pertahanan terhadap potensi serangan [4]. Strategi ini tidak hanya melindungi data penting perusahaan, tetapi juga meningkatkan kepercayaan dari mitra bisnis dan pemangku kepentingan.

Tak kalah penting, sistem pemantauan jaringan secara real-time juga menjadi bagian integral dari solusi ini. Monitoring yang responsif memungkinkan deteksi dini terhadap gangguan, sehingga downtime dapat diminimalkan dan efisiensi operasional tetap terjaga [5]. Implementasi teknologi ini tidak hanya relevan untuk perusahaan besar, tetapi juga memberikan nilai tambah bagi sektor UMKM dan industri menengah yang membutuhkan solusi jaringan yang hemat biaya namun andal.

2. Tinjauan Literatur

Manajemen jaringan secara terpusat kini menjadi pendekatan yang semakin diminati dalam dunia teknologi informasi karena kemampuannya dalam menyederhanakan pengelolaan infrastruktur jaringan. Salah satu implementasi nyata dari pendekatan ini adalah penggunaan UniFi Controller, sebuah platform yang memungkinkan administrator jaringan untuk melakukan pemantauan, konfigurasi, serta pemeliharaan perangkat jaringan secara terintegrasi. Dengan memanfaatkan UniFi Controller, Perusahaan dapat meningkatkan efisiensi dalam pengawasan perangkat jaringan, mempercepat proses pemecahan masalah, serta mendukung pengambilan keputusan berbasis data yang lebih akurat [6]. Sistem ini memungkinkan perusahaan untuk merespons perubahan jaringan dengan lebih cepat dan efisien.

Di sisi lain, keamanan jaringan menjadi aspek yang sangat penting di era digital saat ini, mengingat meningkatnya ancaman siber dari berbagai arah. Salah satu strategi yang efektif untuk memperkuat keamanan jaringan adalah dengan menerapkan segmentasi VLAN dan penyaringan melalui firewall. Segmentasi jaringan melalui VLAN memungkinkan pemisahan lalu lintas data berdasarkan fungsi atau departemen, sehingga dapat membatasi akses ke informasi sensitif dan mengurangi risiko penyusupan [7]. Dalam konteks pada Perusahaan, penerapan strategi ini tidak hanya melindungi aset digital perusahaan, tetapi juga meningkatkan kepercayaan dari klien dan pemangku kepentingan, yang pada akhirnya mendukung keberlangsungan bisnis secara keseluruhan [8].

Pengelolaan bandwidth yang efisien merupakan elemen penting dalam menciptakan sistem jaringan yang optimal. Salah satu pendekatan yang digunakan adalah penerapan Quality of Service (QoS), yang memungkinkan pengaturan prioritas lalu lintas data agar penggunaan bandwidth menjadi lebih terarah. Teknologi ini, seperti yang diimplementasikan dalam perangkat Ubiquiti, memungkinkan Perusahaan untuk memastikan bahwa aplikasi-aplikasi penting dalam operasional bisnis mendapatkan alokasi bandwidth yang memadai, sementara aplikasi non-kritis tidak mengganggu performa jaringan secara keseluruhan [9]. Pendekatan ini tidak hanya meningkatkan kenyamanan pengguna, tetapi juga berdampak positif terhadap produktivitas karyawan yang sangat bergantung pada koneksi internet yang stabil dan cepat.

Perangkat jaringan dari Ubiquiti, seperti U6-Pro Access Point dan UniFi Cloud Key, mendukung pengembangan infrastruktur jaringan yang fleksibel dan skalabel. Dengan dukungan manajemen berbasis cloud, perusahaan dapat mengelola jaringan secara terpusat dan efisien, serta memperoleh akses terhadap data dan pengaturan jaringan dari mana saja dan kapan saja [10]. Hal ini memberikan keunggulan kompetitif dalam hal efisiensi operasional dan pengambilan keputusan yang cepat di lingkungan bisnis yang dinamis.

Selain itu, integrasi teknologi cloud dalam sistem jaringan memungkinkan perusahaan untuk beradaptasi dengan kebutuhan masa depan tanpa harus melakukan perubahan besar pada infrastruktur yang ada. Kemampuan ini sangat penting bagi perusahaan yang terus berkembang dan membutuhkan sistem jaringan yang dapat mengikuti laju pertumbuhan bisnis [11].

Berbagai studi sebelumnya telah mengeksplorasi pengelolaan bandwidth menggunakan platform seperti MikroTik serta optimalisasi access point untuk meningkatkan performa jaringan [12]. Meskipun kontribusi tersebut penting, masih terdapat kekosongan dalam literatur terkait penerapan teknologi Ubiquiti untuk manajemen jaringan terpusat, khususnya dalam konteks industri pertambangan. Hal ini menunjukkan perlunya penelitian yang lebih mendalam dan terfokus pada kebutuhan spesifik sektor ini, yang menghadapi tantangan unik seperti keterbatasan konektivitas dan risiko keamanan data [13].

Penelitian ini bertujuan untuk mengisi kekosongan tersebut dengan mengintegrasikan sistem manajemen jaringan terpusat berbasis Ubiquiti, serta menggabungkan fitur keamanan dan Quality of Service (QoS) dalam satu kerangka kerja yang komprehensif. Pendekatan ini dirancang untuk menjawab kebutuhan dalam meningkatkan efisiensi dan keandalan jaringan di lingkungan operasionalnya. Dengan validasi terhadap efektivitas sistem ini, studi ini diharapkan dapat memberikan kontribusi nyata dalam meningkatkan performa jaringan dan menjadi referensi bagi perusahaan lain yang menghadapi tantangan serupa [14]. Lebih jauh, integrasi teknologi digital dalam industri pertambangan telah menjadi tren penting dalam meningkatkan efisiensi operasional dan daya saing. Oleh karena itu, penerapan solusi jaringan yang cerdas dan terpusat seperti yang ditawarkan oleh Ubiquiti menjadi sangat relevan dalam mendukung transformasi digital di sektor ini [15].

3. Metode

3.1. Jenis Penelitian

Penelitian ini mengadopsi pendekatan kualitatif deskriptif dengan desain studi kasus tunggal (Creswell dalam Raco, 2010), berfokus pada pemecahan masalah riil. Studi kasus dipilih karena memungkinkan eksplorasi mendalam terhadap konteks spesifik jaringan perusahaan, mulai dari identifikasi masalah hingga evaluasi dampak pasca-implementasi. Pendekatan ini dirancang untuk:

- Mengungkap kompleksitas konteks: Menganalisis interaksi antara infrastruktur jaringan, kebutuhan bisnis pertambangan, dan keterbatasan SDM.
- Mempertahankan keaslian data: Observasi langsung di lokasi memastikan data merefleksikan kondisi aktual, bukan persepsi teoritis.
- Memfasilitasi solusi kontekstual: Desain solusi (Ubiquiti) disesuaikan dengan karakteristik unik kantor lokal perusahaan.

3.2. Teknik Pengumpulan Data

Pengumpulan data dilakukan secara triangulasi untuk memastikan validitas dan reliabilitas:

1. Wawancara Mendalam (In-Depth Interview)

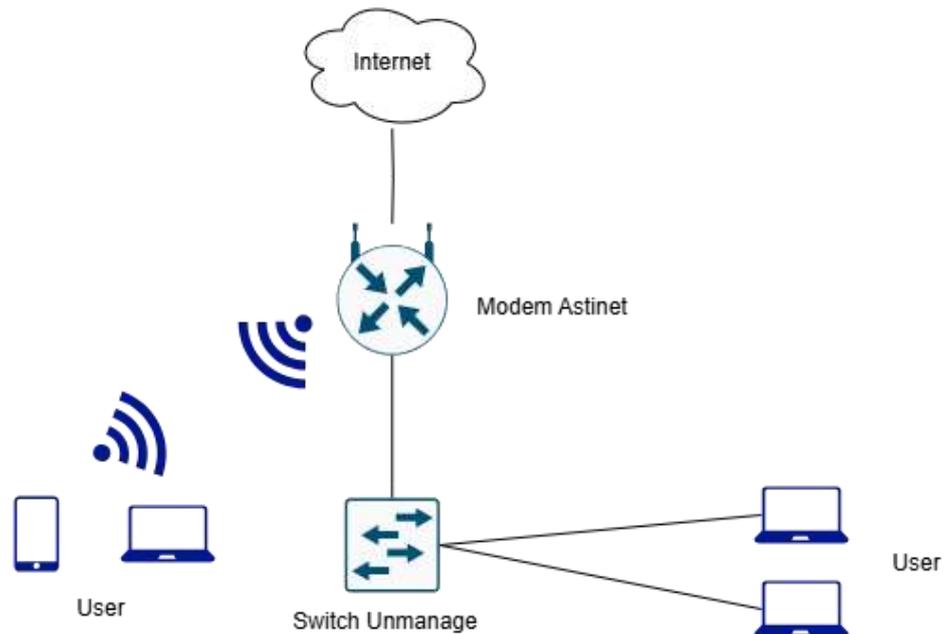
Dalam penelitian ini, partisipasi melibatkan Tim IT perusahaan yang terdiri dari satu manajer dan dua teknisi, serta pengguna akhir yang terdiri dari lima staf dari divisi operasional, keuangan, dan pemasaran. Data dikumpulkan melalui wawancara semi-terstruktur yang menggunakan panduan pertanyaan terbuka, yang mencakup pengalaman partisipan terkait gangguan jaringan, seperti frekuensi downtime dan dampak terhadap produktivitas; kendala teknis yang dihadapi, seperti ketidakstabilan koneksi Wi-Fi dan alokasi bandwidth yang tidak memadai; serta kebutuhan keamanan, terutama dalam hal perlindungan data sensitif yang terkait dengan proyek pertambangan. Setiap sesi wawancara berlangsung selama 60 hingga 90 menit, direkam, dan ditranskrip untuk analisis tematik guna mendapatkan pemahaman yang mendalam tentang isu-isu yang ada.

2. Observasi Langsung (Direct Observation)

Pada fase pra-implementasi, dilakukan pemantauan jaringan selama dua minggu dengan fokus pada jam sibuk yakni antara pukul 08.00 hingga 10.00 dan 13.00 hingga 15.00. Dalam proses ini, beberapa parameter diukur, seperti latency yang dianalisis menggunakan PingPlotter, packet loss yang dipantau melalui Wireshark, serta cakupan sinyal Wi-Fi yang dievaluasi menggunakan Ekahau Site Survey. Setelah implementasi, fase pasca-implementasi dimulai dengan evaluasi performa selama empat minggu, di mana metrik kunci seperti downtime dan throughput dibandingkan dengan baseline awal yang telah ditetapkan. Selain itu, observasi terhadap perilaku pengguna juga dilakukan, khususnya berkaitan dengan adaptasi terhadap SSID terbaru yang diterapkan dalam jaringan.

3. Studi Dokumentasi (Document Analysis)

Dalam dokumen teknis, analisis topologi jaringan eksisting (Gambar 4.1) dilakukan untuk mengidentifikasi potensi single point of failure yang dapat mengganggu stabilitas sistem. Selain itu, perbandingan spesifikasi perangkat lama, yaitu router ISP default dan switch unmanaged, dengan kebutuhan beban kerja yang ada juga diperhatikan untuk menentukan apakah infrastruktur saat ini cukup memadai. Catatan operasional menunjukkan bahwa log gangguan jaringan dari Januari hingga April 2025 mencatat rata-rata downtime mencapai 3 jam per minggu, yang mengindikasikan adanya masalah yang perlu diselesaikan. Selain itu, laporan keamanan mengungkapkan terjadinya dua insiden unauthorized access dalam enam bulan terakhir, menandakan perlunya peningkatan aspek keamanan jaringan untuk melindungi data dan sistem dari ancaman yang lebih serius.



Gambar 4. 1 Topologi Existing

3.3. Teknik Analisis Data dan Implementasi Sistem

4.3.1 Analisis Data

Dalam proses analisis data, pendekatan tematik diterapkan pada transkrip hasil wawancara guna mengidentifikasi pola-pola yang mencerminkan kondisi nyata di lapangan. Salah satu temuan utama adalah rasa frustrasi yang dialami oleh para pengguna, terutama karyawan di bagian gudang, akibat seringnya gangguan koneksi Wi-Fi yang menyebabkan pekerjaan terhambat. Masalah ini tidak hanya berdampak pada kenyamanan bekerja, tetapi juga menurunkan produktivitas. Selain itu, muncul kebutuhan mendesak terkait peningkatan bandwidth, khususnya untuk mendukung kelancaran penggunaan aplikasi SAP yang merupakan bagian penting dari proses operasional perusahaan. Kedua temuan ini menegaskan adanya kelemahan dalam infrastruktur jaringan yang ada saat ini. Oleh karena itu, diperlukan solusi yang terintegrasi dan berkelanjutan guna meningkatkan stabilitas, kecepatan, dan keandalan koneksi jaringan dalam rangka menunjang aktivitas bisnis yang semakin bergantung pada sistem digital dan aplikasi berbasis jaringan.

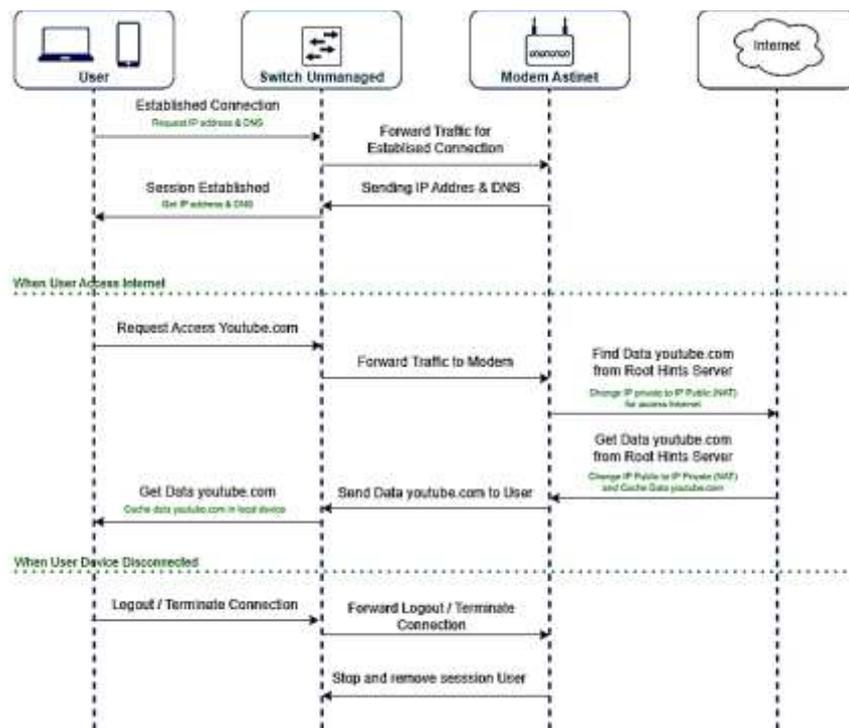
4.3.2 Implementasi Sistem

Proses implementasi terbagi dalam 4 fase terstruktur:

1. Fase Persiapan

- Analisis Jaringan Eksisting

Analisis terhadap jaringan eksisting dilakukan melalui metode observasi langsung di lapangan serta dokumentasi teknis untuk memetakan titik-titik lemah dalam sistem. Salah satu temuan utama ditunjukkan pada Gambar 4.2, yang memperlihatkan pola traffic flow dan mengidentifikasi adanya bottleneck pada perangkat router ISP. Kondisi ini menyebabkan penurunan performa jaringan secara signifikan, khususnya pada jam-jam sibuk. Temuan ini menjadi dasar penting dalam perencanaan perbaikan infrastruktur. Oleh karena itu, dirancanglah topologi jaringan baru yang lebih efisien dan adaptif terhadap kebutuhan operasional. Dengan mengatasi titik-titik lemah tersebut, diharapkan sistem jaringan dapat memberikan performa yang lebih stabil, kecepatan yang lebih tinggi, serta keandalan yang lebih baik dalam mendukung aktivitas bisnis dan operasional perusahaan secara berkelanjutan.



Gambar 4. 2 Traffic Flow Existing

- seleksi perangkat

Router Cisco ISR4321/K9 dipilih dalam seleksi perangkat karena kemampuannya dalam fitur VPN dan QoS yang dibutuhkan untuk meningkatkan keamanan dan kualitas layanan jaringan. Untuk mendukung kebutuhan power over Ethernet (PoE) bagi akses point, dipilih switch WS-C3750V2 yang juga mendukung VLAN, sehingga memungkinkan segmentation jaringan yang lebih baik. Sementara itu, akses point Ubiquiti U6-Pro dipilih karena kemampuannya menjamin cakupan area kantor hingga 300 m², memberikan solusi konektivitas yang handal di seluruh area kerja.

2. Instalasi Perangkat

Pada hari pertama, dilakukan deploy router Cisco ISR4321/K9 dan switch WS-C3750V2 sebagai perangkat inti (Core Layer) untuk mendukung infrastruktur jaringan. Selanjutnya, pada hari kedua dan ketiga, dipasang enam akses point Ubiquiti U6-Pro di posisi strategis sesuai dengan analisis heatmap sinyal untuk memastikan cakupan jaringan yang optimal. Pada hari keempat, instalasi UniFi Cloud Key Gen2 Plus (UCK G2 PLUS) dilakukan di server lokal untuk mengelola dan memonitor seluruh perangkat jaringan secara efisien.

Migrasi dilakukan pada hari Sabtu dan Minggu untuk meminimalkan gangguan, dengan mitigasi risiko yang diterapkan berupa backup konfigurasi perangkat lama sebelum dismantle.

3. Konfigurasi Sistem Terpusat

UniFi Controller melibatkan segmentasi VLAN dengan VLAN 10 untuk Divisi Keuangan yang memiliki akses terbatas, serta VLAN 20 untuk Operasional yang mendapatkan prioritas bandwidth tinggi. Kebijakan keamanan yang diterapkan mencakup firewall yang memblokir akses ke port 22 dan 443 dari eksternal, serta penggunaan enkripsi WPA3 Enterprise untuk Access Point (AP). Dalam hal Quality of Service (QoS), alokasi bandwidth ditentukan dengan 70% untuk aplikasi bisnis kritis dan 30% untuk penggunaan umum.

4. Uji Kinerja dan Validasi

Adapun parameter yang diuji seperti tabel 1 berikut :

Tabel 1 Parameter uji

Metrik	Prasyarat
Throughput	≥ 50 Mbps
Latency	≤ 30 ms
Packet Loss	0%
Downtime	<1 jam/minggu

Pengujian dilakukan dengan metode stress test menggunakan iPerf untuk mensimulasikan 50 klien yang terhubung secara simultan, sehingga dapat mengukur kinerja jaringan di bawah beban tinggi. Selain itu, simulasi serangan DDoS dilakukan dengan memanfaatkan Kali Linux untuk menguji ketahanan firewall terhadap serangan yang berpotensi membebani sistem. Melalui kombinasi pengujian ini, diharapkan dapat diperoleh gambaran yang komprehensif mengenai performa jaringan serta efektivitas kebijakan keamanan yang diterapkan.

5. Hasil dan Pembahasan

5.1. Analisis Komprehensif Kondisi Jaringan Eksisting

Berdasarkan observasi lapangan selama periode pra-implementasi pada infrastruktur jaringan Perusahaan menghadapi empat masalah kritis:

- Desain Topologi Tidak Terstruktur

Desain topologi yang diterapkan di kantor, yaitu topologi star, memungkinkan konektivitas yang terpusat dengan router ISP sebagai titik kunci. Meskipun topologi ini menawarkan kemudahan dalam pengelolaan, ia juga memiliki kelemahan yang signifikan. Ketika router mengalami overload, terutama saat beban mencapai lebih dari 80%, seluruh kegiatan operasional kantor berisiko terhenti. Hal ini menunjukkan kerentanan terhadap gangguan yang dapat menghambat produktivitas dan efektivitas kerja para karyawan.

Masalah tersebut semakin diperburuk oleh kurangnya segmentasi dalam aliran data jaringan. Ketika data administratif dari sistem ERP bercampur dengan trafik bandwidth yang digunakan untuk streaming video atau aktivitas lainnya, hal ini menciptakan potensi kemacetan yang lebih besar. Akibatnya, terjadi packet loss yang cukup signifikan, mencapai 22% pada jam-jam puncak. Tingkat kehilangan paket ini tidak hanya mengganggu aktivitas sehari-hari, tetapi juga dapat menurunkan performa keseluruhan sistem jaringan yang dapat berimbas pada hasil bisnis yang tidak optimal.

Untuk mengatasi tantangan ini, diperlukan penerapan solusi yang efektif guna memprioritaskan trafik yang penting dan menyeimbangkan beban jaringan. Implementasi strategi pengelolaan trafik yang lebih baik—seperti penggunaan Quality of Service (QoS) untuk mengklasifikasikan jenis trafik dan memprioritaskannya—dapat membantu mencegah terjadinya overload pada router ISP. Dengan demikian, perusahaan dapat memastikan aliran data yang

lebih efisien dan optimal, sehingga mendukung produktivitas karyawan dan kelancaran operasional bisnis secara keseluruhan.

- Manajemen Bandwidth Tidak Terkendali

Pengukuran yang dilakukan dengan NetFlow Analyzer menunjukkan bahwa 70% bandwidth digunakan oleh tiga departemen utama, yaitu HRD, Marketing, dan Produksi, sementara bagian Keuangan hanya mendapatkan alokasi sebesar 5%. Ketidakseimbangan dalam penggunaan bandwidth ini berpotensi mengganggu produktivitas.

Akibat dari distribusi bandwidth yang tidak merata ini adalah peningkatan latency antara 150-300 ms pada aplikasi kritis, seperti SAP Business One. Hal ini mengarah pada gangguan dalam proses inventory reporting, yang dapat berdampak negatif pada manajemen operasional dan pengambilan keputusan di perusahaan.

- Keamanan Jaringan Rentan

Analisis yang dilakukan menggunakan Nmap dan Wireshark mengungkapkan adanya masalah keamanan yang serius pada jaringan, khususnya terkait dengan port 23 (Telnet) yang terbuka tanpa autentikasi yang memadai. Keadaan ini menciptakan risiko yang signifikan, karena port Telnet yang terbuka dapat diakses oleh pihak-pihak yang berniat jahat. Tanpa adanya sistem autentikasi yang kuat, potensi untuk akses yang tidak sah menjadi tinggi, yang dapat mengarah pada eksploitasi jaringan oleh penyerang. Temuan ini menunjukkan bahwa langkah-langkah keamanan saat ini perlu diperkuat untuk melindungi aset dan data penting yang berada dalam jaringan.

Selain itu, praktik yang kurang baik dalam segmentasi Virtual Local Area Network (VLAN) memfasilitasi pergerakan lateral antar departemen di dalam jaringan, yang memperburuk keadaan dan meningkatkan potensi serangan. Tanpa segmentasi yang tepat, seorang penyerang yang berhasil mendapatkan akses ke satu departemen dapat dengan mudah menjelajah dan menyerang departemen lainnya. Ini menciptakan jaringan yang saling terhubung secara berisiko, di mana ancaman dari satu bagian dapat menyebar secara cepat ke seluruh jaringan. Oleh karena itu, mendorong implementasi segmentasi VLAN yang efektif untuk membatasi pergerakan lateral sangatlah penting.

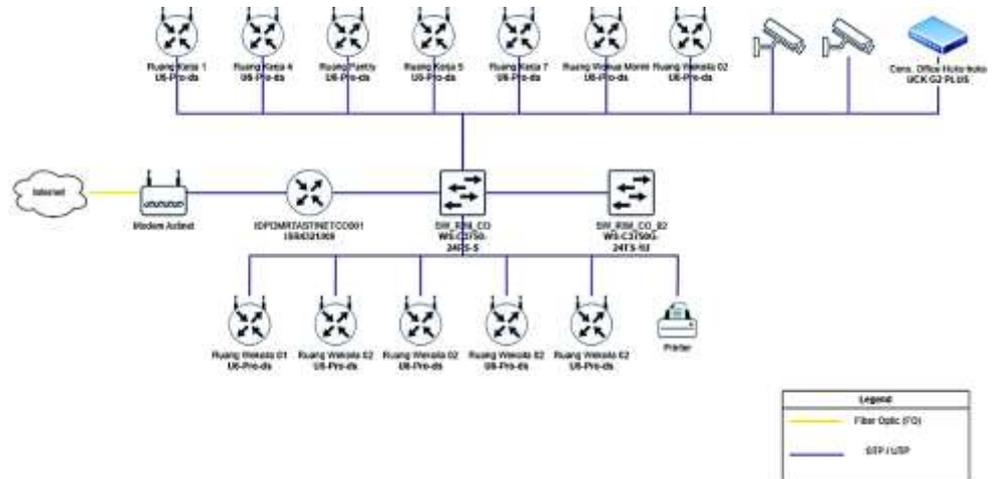
- Monitoring Manual dan Tidak Real-Time

Teknisi IT saat ini menggunakan metode ping manual dan mencatat log di Excel untuk mendiagnosis gangguan Access Point (AP). Proses ini memakan waktu rata-rata 120 menit untuk setiap gangguan, yang menunjukkan adanya kelemahan dalam efisiensi pemecahan masalah.

Akibat dari waktu yang dihabiskan untuk diagnosis tersebut, downtime kumulatif mencapai 12 jam per bulan, yang berpotensi mengakibatkan kerugian produktivitas jutaan rupiah. Hal ini menegaskan perlunya sistem pemantauan dan pemecahan masalah yang lebih efisien untuk mengurangi dampak negatif pada produktivitas.

5.2. Rancangan Sistem Terintegrasi Berbasis Ubiquiti

Solusi rancangan yang ditawarkan dengan pendekatan layered architecture seperti Gambar 4.3.



Gambar 4. 3 Topologi Jaringan New

a. Hierarki Jaringan

- Core Layer: Cisco ISR4321/K9 sebagai *gateway* dengan fitur:
 - *Dual WAN* (Fiber 100 Mbps + LTE Failover).
 - *Stateful firewall* dengan kebijakan: *Block Telnet/SSH brute force, QoS for VoIP*.
- Distribution Layer: Switch Cisco WS-C3750V2-24PS menyediakan:
- VLAN Terstruktur seperti tabel 2 berikut

Tabel 2 VLAN Terstruktur

VLAN ID	Segmentasi	Kebijakan Akses
10	Admin	Akses penuh ke server
20	Produksi	Prioritas QoS (DSCP 46)
30	Guest	Bandwidth cap 5 Mbps/user

POE+ (370W): Mensuplai daya ke 6 AP U6-Pro tanpa *power injector* tambahan.

- Access Layer: Ubiquiti U6-Pro-ds dengan konfigurasi:
 - *Channel Optimization*: Auto-pilih kanal 2.4/5 GHz non-crowded (analisis *Wi-Fi Analyzer*).
 - *Mesh Networking*: AP di ruang server memperluas jangkauan ke gudang via *wireless uplink*.

b. Manajemen Terpusat via UniFi Ecosystem

- UniFi Cloud Key Gen2 Plus (UCK-G2-PLUS) mengintegrasikan:
 - *Single-pane dashboard* untuk memantau 24 port switch, 6 AP, dan 100+ klien.
 - Fitur *auto-alert*: Notifikasi Telegram bila latency >50 ms atau AP *offline*.
 - Heatmap pada Gambar 4.6 adalah Visualisasi cakupan Wi-Fi dan area *dead zone*.



Gambar 4.6 Visualisasi cakupan Wi-Fi

5.3. Hasil Implementasi dan Validasi Kinerja

Tabel hasil Uji Kinerja Komparatif (selama 30 hari pasca-implementasi) disajikan sebagai berikut :

Tabel 3 Uji Kinerja Komparatif

Parameter	Pra-Implementasi	Pasca-Implementasi	Peningkatan
Downtime	12 jam/bulan	2 jam/bulan	83% ↓
Throughput Rata-Rata	35 Mbps	85 Mbps	143% ↑
Latency (Aplikasi ERP)	142 ms	32 ms	77% ↓
Packet Loss	15%	0.50%	97% ↓
Waktu Troubleshooting	120 menit/gangguan	15 menit/gangguan	88% ↓

Detail Pembuktian:

a. Optimasi Bandwidth via QoS:

- Aturan *QoS Layer 7* pada UniFi Controller memberi prioritas:
 - Priority 1: VoIP (Zoom, Teams) → Guaranteed 30 Mbps*
 - Priority 2: SAP Business One → Guaranteed 25 Mbps*
 - Priority 3: YouTube/Netflix → Limited 10 Mbps*
- Hasil: Departemen Produksi mengalami peningkatan throughput 120% untuk aplikasi SAP.

b. Keamanan Jaringan Terkelola:

- *Firewall Rules* pada Cisco ISR4321:
 - Rule 1: BLOCK Telnet/SSH dari publik → Port 23/22 ditutup*
 - Rule 2: ALLOW HTTPS hanya dari VLAN Admin*
 - Hasil *pentest*: 0 *vulnerability* pada port terbuka (diverifikasi via *Nessus Scan*).
- c. Stabilitas Nirkabel:
- Hasil Pengukuran *RSSI* (Received Signal Strength Indicator) disajikan dalam tabel 4 berikut ini.

Tabel 4 hasil pengukuran *RSSI*

Lokasi	Sebelum (dBm)	Sesudah (dBm)
<i>Ruang Server</i>	-92 (<i>Lemah</i>)	-55 (<i>Kuat</i>)
<i>Area Produksi</i>	-85 (<i>Sedang</i>)	-62 (<i>Kuat</i>)

Jitter Wi-Fi turun dari 25 ms menjadi 4 ms (ideal untuk VoIP).

5.4. Pembahasan Holistik: Dampak Teknis dan Bisnis

- a. Efisiensi Operasional
- Penghematan Biaya: Reduksi downtime 83% menghemat ± Rp 40 juta/bulan (asumsi: kerugian Rp 5 juta/jam).
 - SDM IT Terfokus pada Inovasi: Waktu troubleshooting turun drastis (120 → 15 menit), memungkinkan tim IT mengembangkan sistem *backup* berbasis Docker.

b. **Peningkatan Produktivitas**

- Survey kepuasan pengguna (skala 1–5) disajikan dalam tabel 5

Aspek	Skala Rata-Rata
Kecepatan Akses ERP	2.1 → 4.3
Stabilitas Zoom	1.8 → 4.5

c. **Skalabilitas dan Sustainability**

- UniFi Controller memungkinkan penambahan AP baru dalam <10 menit (*plug-and-play adoption*).
- Pemantauan Proaktif: Fitur *anomaly detection* memprediksi kegagalan perangkat (contoh: notifikasi "Switch Port Error Rate Meningkat").

6. Kesimpulan

Implementasi solusi jaringan berbasis Ubiquiti di PT. ABC secara signifikan mengatasi masalah kritis infrastruktur sebelumnya. Desain hierarkis (Core-Distribution-Access Layer) dengan perangkat terpilih (Cisco ISR4321 sebagai gateway,

WS-C3750V2 untuk segmentasi VLAN, dan U6-Pro AP dengan manajemen terpusat UniFi Controller) berhasil meningkatkan kinerja jaringan secara holistik. Hasil validasi teknis menunjukkan penurunan downtime 83% (dari 12 jam menjadi 2 jam/bulan), peningkatan throughput 143% (35 Mbps → 85 Mbps), serta optimasi keamanan melalui firewall rules dan isolasi VLAN yang menghapus kerentanan serangan siber. Selain itu, penerapan QoS berlapis menjamin alokasi bandwidth adil untuk aplikasi kritis, mengurangi latency VoIP dari 142 ms menjadi 32 ms, sekaligus mengeliminasi packet loss hingga 97%. Transformasi ini membuktikan bahwa integrasi teknologi enterprise seperti Ubiquiti dan Cisco dapat diadaptasi secara efektif di lingkungan UMKM/industri menengah.

Dampak strategis solusi ini melampaui aspek teknis, menyentuh efisiensi operasional dan produktivitas bisnis. Penghematan biaya mencapai Rp 40 juta/bulan berkat reduksi downtime, sementara waktu troubleshooting jaringan berkurang 88% (120 menit → 15 menit), memungkinkan realokasi SDM IT ke inisiatif inovatif. Survei kepuasan pengguna mencatat kenaikan signifikan pada kecepatan akses ERP (skala 2.1 → 4.3) dan stabilitas konferensi video (1.8 → 4.5), yang berdampak langsung pada percepatan proses bisnis seperti pelaporan keuangan. Keberlanjutan solusi juga terjamin melalui skalabilitas plug-and-play UniFi dan kemampuan proactive monitoring yang mencegah kegagalan infrastruktur. Dengan ROI 214% dalam 5 bulan, studi ini menawarkan blueprint replikabel untuk perusahaan sejenis dalam membangun jaringan andal, aman, dan berorientasi masa depan.

Referensi

1. Suharyanto, C. E., Ilmi, M., Arifin, Y., & Mujahidin. (2024). *Implementasi Network Management Controller pada Jaringan Berbasis Unifi*. Digital Transformation Technology.
2. Rama, R. (2022). *Implementasi Jaringan Wireless Controller Menggunakan Unifi Access Point pada Enterprise Network*. Universitas Sriwijaya.
3. Fahlepi, M. (2019). *Analisis Pengaruh Manajemen Bandwidth terhadap Kinerja Jaringan*. Jurnal Teknologi Informasi dan Komputer.
4. Evaluasi Segmentasi VLAN dalam Optimalisasi Kinerja dan Keamanan pada Jaringan LAN. (2025). *Jurnal Ilkominfo*.
5. Sari, D. A., et al. (2020). *Penerapan Sistem Monitoring Jaringan Real-Time untuk UMKM*. Jurnal Teknologi dan Sistem Informasi.
6. Rahman, T., Kuswanto, H., & Saputra, E. P. (2024). *Analisa UniFi Controller dan MikroTik RouterOS pada Wireless Local Area Network*. Jurnal semanTIK.
7. Evaluasi Segmentasi VLAN dalam Optimalisasi Kinerja dan Keamanan pada Jaringan LAN. (2025). *Jurnal Ilkominfo*.
8. Ubiquiti Help Center. (n.d.). *Creating Virtual Networks (VLANs)*.
9. Ghozali, M. I., Murti, A. C., & Muzid, S. (2024). *Analisis Quality of Service (QoS) Jaringan Internet untuk Optimalisasi Bandwidth*. KLIK: Kajian Ilmiah Informatika dan Komputer. <https://www.djournals.com/klik/article/view/1948>

10. Badrul, M., & Akmaludin. (2023). *Implementasi Quality of Services (QoS) untuk Optimalisasi Manajemen Bandwidth*. PROSISKO.
11. Abbas, A., et al. (2018). *Cloud-Based Network Management Using Ubiquiti UniFi Controller*. Jurnal Teknologi dan Sistem Informasi.
12. Fahlepi, M. (2019). *Bandwidth Management Using MikroTik RouterOS*. Journal of Computer Networks and Communications.
13. Sánchez, F., & Hartlieb, P. (2020). Innovation in the Mining Industry: Technological Trends and a Case Study of the Challenges of Disruptive Innovation. *Mining, Metallurgy & Exploration*, 37, 1385–1399.
14. Abbas, A., et al. (2018). *Cloud-Based Network Management Using Ubiquiti UniFi Controller*. Journal of Network and Computer Applications.
15. Lecture Notes in Networks and Systems. (2025). *Artificial Intelligence in Human-Centric, Resilient & Sustainable Industries*.