

BAB III

ANALISA JARINGAN BERJALAN

3.1. Tinjauan Perusahaan

PT. ABB Sakti Industri merupakan perusahaan manufaktur yang berfokus pada produksi dan distribusi peralatan listrik serta sistem *otomasi* industri. Perusahaan ini merupakan bagian dari ABB Group, sebuah korporasi multinasional yang berkantor pusat di Zurich, Swiss, dan beroperasi di lebih dari 100 negara. ABB dikenal sebagai pemimpin global dalam teknologi kelistrikan dan *otomasi*, yang berfokus pada efisiensi energi dan produktivitas industri.

3.1.1. Sejarah Perusahaan

PT. ABB Sakti Industri didirikan pada tahun 1990 dan berlokasi di kawasan industri Cibitung, Bekasi, Jawa Barat. Sejak awal pendiriannya, perusahaan ini berkomitmen untuk menyediakan solusi teknologi yang inovatif dan berkelanjutan bagi sektor industri di Indonesia. Dalam operasionalnya, perusahaan sangat bergantung pada sistem jaringan komputer yang *handal* untuk mendukung proses produksi, pengawasan mutu, logistik, serta komunikasi internal dan eksternal.

Seiring perkembangan teknologi dan meningkatnya kebutuhan akan konektivitas yang andal, PT. ABB Sakti Industri terus melakukan pembaruan pada infrastruktur jaringannya. Salah satu tantangan utama adalah menjaga kestabilan dan ketersediaan koneksi internet tanpa gangguan, terutama karena perusahaan memanfaatkan dua jalur ISP untuk mendukung operasionalnya. Oleh karena itu, diperlukan sistem manajemen jaringan yang mampu mengatur beban lalu lintas data

secara efisien dan menyediakan cadangan koneksi secara otomatis saat terjadi gangguan.

3.1.2. Struktur Organisasi dan Fungsi

Struktur organisasi PT. ABB Sakti Industri disusun secara sistematis untuk mengoptimalkan efisiensi serta efektivitas koordinasi dan pelaksanaan tugas antar divisi. Adapun struktur organisasi secara umum terdiri dari:

1. Direktur Utama

Memiliki tanggung jawab dalam menetapkan keputusan strategis serta melakukan pengawasan menyeluruh terhadap seluruh aktivitas operasional perusahaan.

2. Divisi Teknologi Informasi (IT)

Bertugas mengelola infrastruktur jaringan komputer, *server*, sistem keamanan jaringan, serta mendukung kebutuhan teknologi informasi seluruh divisi.

3. Divisi Produksi

Bertanggung jawab terhadap pengelolaan proses manufaktur, pengendalian kualitas, serta pemeliharaan peralatan produksi.

4. Divisi Logistik dan Gudang

Memiliki tanggung jawab dalam pengelolaan distribusi barang, manajemen penyimpanan, serta pelaksanaan pengiriman produk kepada pelanggan.

5. Divisi Keuangan dan Administrasi

Menjalankan fungsi manajemen keuangan, pengelolaan sistem penggajian, dan koordinasi administrasi perusahaan.

6. Divisi Sumber Daya Manusia (SDM)

Bertanggung jawab atas proses rekrutmen, pelaksanaan program pelatihan, serta pengembangan kompetensi karyawan.

Divisi Teknologi Informasi berperan strategis dalam memastikan stabilitas dan keamanan infrastruktur jaringan perusahaan. Mengingat tingginya jumlah pengguna serta kebutuhan konektivitas yang besar, diperlukan sistem manajemen jaringan yang mampu menjamin ketersediaan layanan internet secara optimal dan berkesinambungan. Oleh karena itu, implementasi metode *load balancing* dan *failover* berbasis Mikrotik menjadi solusi yang relevan untuk meningkatkan performa dan keandalan jaringan di lingkungan PT. ABB Sakti Industri.

3.2. Skema Jaringan Berjalan

3.2.1. Topologi Jaringan

Topologi jaringan yang digunakan di PT. ABB Sakti Industri saat ini adalah topologi *hybrid*, yang menggabungkan model *star* dan *extended star*. Semua perangkat *client* terhubung ke *switch* utama yang kemudian terhubung ke *router* Mikrotik sebagai pusat pengendali lalu lintas jaringan. *Router* ini juga terhubung ke dua jalur internet dari dua ISP berbeda, namun hanya satu jalur yang aktif secara *default*.

Topologi ini dipilih karena fleksibel dan mudah dalam pengelolaan, namun belum optimal dalam hal *redundansi* dan distribusi beban koneksi internet.

3.2.2. Arsitektur Jaringan

Arsitektur jaringan pada PT ABB Sakti Industri dirancang untuk mendukung operasional bisnis yang membutuhkan konektivitas stabil, aman, serta mampu menangani beban komunikasi data antar unit kerja. Infrastruktur jaringan dibangun dengan pendekatan berlapis sesuai standar industri, meliputi penggunaan IP Address yang terstruktur, implementasi model referensi OSI/TCP-IP, konfigurasi Domain Name System (DNS), serta dukungan Quality of Service (QoS) untuk menjaga performa layanan.

1. IP Addressing

PT. ABB Sakti Industri menggunakan skema IP *Private* sebagaimana direkomendasikan oleh RFC 1918. Pembagian segmen IP dilakukan berdasarkan kebutuhan fungsi dan lokasi agar lebih mudah dalam manajemen jaringan, *monitoring*, dan pengamanan.

Tabel III.1 IP Address Berdasarkan Kebutuhan Fungsi

VLAN / Departemen	Subnet	Fungsi
VLAN 10 – Office User	10.129.10.0/24	Akses user kantor dan workstation
VLAN 20 – Engineering	10.129.20.0/24	Device engineering, PC konfigurasi sistem
VLAN 30 – Server Farm	10.129.30.0/24	Server aplikasi internal dan database
VLAN 40 – Printer	10.129.40.0/24	Printer network dan perangkat shared
VLAN 50 – CCTV & IoT	10.129.50.0/24	Kamera pengawasan dan perangkat IoT

Sumber: Divisi IT PT ABB

Penataan IP *Address* yang tersegmentasi mendukung isolasi trafik, mengurangi risiko broadcast storm, serta mempermudah penerapan kebijakan keamanan (ACL dan firewall filtering).

2. Model Arsitektur OSI dan TCP/IP

Arsitektur jaringan di perusahaan mengacu pada dua model utama yaitu:

a. Model Lapisan OSI

“Model arsitektur jaringan yang disebut *Open System Interconnection* (OSI) telah dikembangkan oleh ISO dan terdiri dari tujuh lapisan. Setiap lapisan memiliki tanggung jawabnya sendiri, seperti pengalamatan, kontrol aliran, kontrol kesalahan, enkapsulasi, dan transfer pesan yang andal.” [26]

Tujuh lapisan dari model OSI yaitu:

1) *Physical Layer*

“Karakteristik fisik media transmisi, termasuk konektor, pin, penggunaan pin, arus listrik, pengkodean, modulasi cahaya, dan aspek-aspek lainnya didefinisikan oleh lapisan ini.” [26]

2) *Data Link Layer*

“Protokol untuk mengirimkan data melalui satu jenis jaringan fisik tertentu, contohnya protokol tautan data Ethernet, ditentukan oleh lapisan ini. [26]

3) *Network Layer*

“Lapisan ini fokus pada aspek pengalamatan logis, perutean (penerusan), dan protokol perutean yang digunakan untuk mempelajari rute.” [26].

4) *Transport Layer*

“Lapisan ini ditujukan untuk pengiriman data antara dua host titik akhir dan menangani pemulihan kesalahan.” [26]

5) *Session Layer*

“Lapisan ini menyusun pesan dua arah ke dalam alur kerja untuk manajemen yang lebih mudah dan kemampuan mundur dari pekerjaan yang terjadi jika seluruh alur kerja gagal.” [26]

6) *Presentation Layer*

“Lapisan ini berperan dalam menegosiasikan format data, seperti teks ASCII, atau jenis gambar seperti JPEG.” [26]

7) *Application Layer*

“Lapisan ini memberikan antarmuka dari aplikasi ke jaringan dengan menyediakan protokol yang memiliki arti bagi aplikasi.” [26]

b. Model TCP/IP

digunakan sebagai model praktis implementasi jaringan. Empat lapisan utamanya:

- 1) Network Access Layer – interface ethernet dan VLAN.
- 2) Internet Layer – IP Addressing dan protokol routing.
- 3) Transport Layer – implementasi TCP untuk komunikasi andal serta UDP untuk aplikasi real-time.
- 4) Application Layer – DNS, DHCP, HTTP/HTTPS, dan layanan internal perusahaan.

3. *Domain Name System (DNS)*

Domain Name System (DNS) adalah sistem yang digunakan untuk menerjemahkan nama domain yang mudah diingat menjadi alamat IP numerik yang digunakan oleh komputer dalam jaringan. DNS berfungsi sebagai direktori atau penerjemah yang menghubungkan nama domain, seperti *www.contoso.com*, dengan alamat IP yang sesuai, seperti 192.168.1.1. Dengan adanya DNS, pengguna dapat mengakses situs web atau layanan online menggunakan nama domain yang lebih mudah diingat tanpa perlu mengingat alamat IP yang rumit. DNS memainkan peran

penting dalam fungsi internet dan navigasi online. Domain dari PT. ABB Sakti Industri adalah abb.com.

4. *Quality of Service (QoS)*

Untuk menjaga performa khususnya pada aplikasi *real-time* seperti *Microsoft Teams meeting, VoIP*, serta koneksi antar sistem produksi diterapkan kebijakan QoS pada switch dan router. Implementasi QoS meliputi:

a. *Traffic Prioritization (Priority Queueing)*

Memberikan prioritas tinggi untuk trafik voice dan video conference.

b. *Bandwidth Management (Rate Limiting & Shaping)*

Membatasi aplikasi yang tidak kritis agar tidak mengganggu trafik utama.

c. *Class of Service (CoS) dan Differentiated Services (DiffServ/DSCP)*

Menandai paket data berdasarkan jenis trafik.

Tabel III.2 DSCP Yang Digunakan

Layanan	DSCP	Prioritas
Voice / VoIP	EF (46)	Tinggi
Video (Teams/Zoom)	AF41	Menengah Tinggi
Data aplikasi ERP	AF21	Menengah
Traffic umum	BE (0)	Normal

Sumber : Divisi IT PT ABB

5. Fungsi arsitektur jaringan di PT. ABB Sakti Industri

Arsitektur jaringan memiliki beberapa fungsi fundamental untuk menjaga keberlangsungan sistem komunikasi dalam perusahaan:

a. Menentukan alur *trafik* data

Arsitektur mengatur bagaimana paket berpindah dari sumber ke tujuan melalui *router*, *switch*, dan protokol *routing* yang sesuai.

b. Menjamin keandalan dan redundansi

Sistem seperti *load balancing*, *failover*, dan *link backup* memastikan jaringan tetap berfungsi meskipun terjadi gangguan pada salah satu jalur komunikasi.

c. Meningkatkan keamanan jaringan

Melalui segmentasi VLAN, *firewall*, NAT, *filtering*, dan *access control list* (ACL), arsitektur jaringan melindungi data dari ancaman internal maupun eksternal.

d. Mendukung perluasan dan skalabilitas

Arsitektur yang baik memungkinkan penambahan perangkat, server, maupun subnet tanpa mengganggu operasi yang sudah berjalan.

e. Memudahkan manajemen dan *troubleshooting*

Dengan struktur pengalamatan dan dokumentasi yang terstandarisasi, pengelolaan jaringan dan proses pemecahan masalah dapat dilakukan lebih cepat dan akurat.

6. Network Address Translation (NAT)

Teknologi NAT yang digunakan dalam jaringan komputer untuk mengonversi alamat IP privat di dalam jaringan lokal menjadi alamat IP publik yang dapat digunakan di internet. Hal ini memungkinkan beberapa perangkat dalam suatu jaringan lokal untuk berbagi satu alamat IP publik ketika terhubung ke internet. NAT

membantu mengatasi keterbatasan jumlah alamat IP publik yang tersedia dan memberikan tingkat keamanan karena alamat IP internal tidak langsung terlihat dari luar jaringan. Dengan NAT, data yang dikirimkan dari perangkat dalam jaringan lokal dapat dikonversi dan diteruskan melalui satu alamat IP publik, dan respon dari *server* di internet kemudian dikonversi kembali ke alamat IP internal yang sesuai. PT. ABB Sakti Industri menggunakan teknologi NAT untuk memberikan akses internet kepada penggunanya.

7. Firewall

Firewall dapat didefinisikan sebagai suatu sistem keamanan yang digunakan untuk melindungi jaringan komputer dari akses atau serangan yang tidak sah dari luar. Fungsinya adalah mengontrol dan memonitor lalu lintas data yang masuk dan keluar dari jaringan, serta menentukan apakah data tersebut diperbolehkan atau diblokir berdasarkan aturan keamanan yang telah ditetapkan. Firewall dapat berupa perangkat keras (*hardware*) atau perangkat lunak (*software*) yang diimplementasikan pada jaringan untuk mencegah akses yang tidak diinginkan atau potensi serangan dari pihak luar. *Firewall* yang digunakan oleh PT. ABB Sakti Industri adalah Zscaler.

8. Internet Service Provider (ISP)

Internet Service Provider (ISP) merupakan rancangan yang menentukan bagaimana konektivitas internet diintegrasikan ke dalam infrastruktur jaringan perusahaan. Pada lingkungan operasional seperti PT ABB Sakti Industri, keberadaan lebih dari satu ISP menjadi kebutuhan penting untuk memastikan ketersediaan layanan

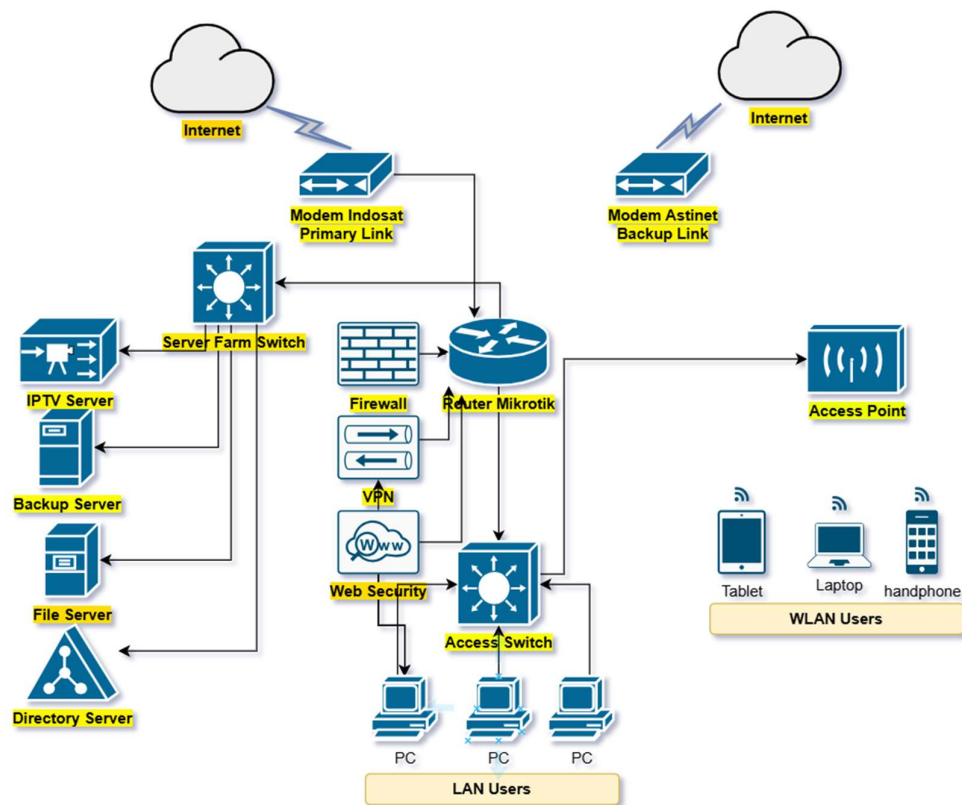
(*availability*), kontinuitas operasional, serta meminimalisir risiko gangguan akibat kegagalan koneksi dari satu penyedia layanan. ISP yang digunakan oleh PT. ABB Sakti Industri adalah ISP Indosat sebagai jalur utama dan ISP Astinet sebagai jalur cadangan.

3.2.3. Skema Jaringan

Skema jaringan menunjukkan bahwa koneksi dari kedua ISP masuk ke *router* Mikrotik, namun hanya satu jalur yang digunakan secara aktif. *Router* kemudian mendistribusikan koneksi ke *switch* utama, yang selanjutnya menghubungkan ke seluruh perangkat *client* di kantor pusat dan area produksi. Tidak terdapat sistem otomatisasi untuk *failover* atau pembagian beban (*load balancing*), sehingga jika ISP utama mengalami gangguan, koneksi harus dialihkan secara manual oleh tim IT. Berikut adalah diagram skema jaringan berjalan:



UNIVERSITAS
NUSA MANDIRI



Sumber: Hasil Penelitian

Gambar III.1 Skema Jaringan Berjalan

3.2.4. Keamanan Jaringan

Keamanan jaringan saat ini masih bersifat dasar. *Router* Mikrotik hanya menggunakan *firewall* standar dengan beberapa *rule* dasar seperti pemblokiran *port* tertentu dan NAT. Belum ada sistem deteksi intrusi (IDS), segmentasi VLAN, atau *otentikasi* pengguna berbasis server. Hal ini menyebabkan jaringan rentan terhadap serangan dari luar maupun kesalahan konfigurasi internal.

3.2.5. Spesifikasi Hardware dan *Software* Jaringan

Berikut adalah spesifikasi perangkat keras dan lunak yang digunakan dalam jaringan saat ini:

Tabel III.3 Spesifikasi Hardware dan Software Jaringan

Komponen	Spesifikasi
<i>Router</i>	Mikrotik RB4011iGS+RM
ISP	ISP A (100 Mbps), ISP B (50 Mbps)
<i>Switch</i>	Cisco <i>Catalyst</i> 2960
Server	Dell <i>PowerEdge</i> R540, Ubuntu Server 22.04 LTS
<i>Client</i>	±50 unit PC, Windows 10 Pro
<i>Firewall</i>	Mikrotik <i>Firewall (basic rules)</i>
<i>Monitoring</i>	Belum tersedia
Topologi	<i>Hybrid (Star + Extended Star)</i>

Sumber: Divisi IT PT ABB

3.3. Permasalahan

Dalam proses analisa terhadap jaringan komputer yang berjalan di PT. ABB Sakti Industri, ditemukan sejumlah permasalahan yang berdampak pada performa, efisiensi, dan keandalan jaringan. Permasalahan ini muncul baik dari sisi teknis maupun manajerial, yang secara keseluruhan dapat menghambat kelancaran operasional perusahaan. Adapun permasalahan yang diidentifikasi adalah sebagai berikut:

1. Pemanfaatan Jalur Internet Tidak Optimal. Meskipun perusahaan memiliki dua jalur koneksi internet dari dua ISP berbeda, hanya satu jalur (ISP A) yang digunakan secara aktif. Jalur ISP B hanya difungsikan saat terjadi gangguan pada ISP A, dan proses peralihannya dilakukan secara manual.

Hal ini menyebabkan potensi *bandwidth* dari ISP B tidak dimanfaatkan secara maksimal.

2. Tidak Tersedianya Sistem *Load Balancing*. Seluruh *trafik* internet dibebankan pada satu jalur ISP tanpa adanya pembagian beban (*load balancing*). Akibatnya, saat terjadi lonjakan *trafik*, koneksi menjadi lambat dan tidak stabil. Padahal, dengan metode *load balancing*, beban dapat dibagi secara merata ke dua jalur ISP sehingga performa jaringan lebih optimal.

3. *Failover* Manual dan Tidak Otomatis. Ketika ISP utama mengalami gangguan, proses pengalihan koneksi ke ISP cadangan dilakukan secara manual oleh tim IT. Proses ini memerlukan waktu dan keahlian teknis, yang menyebabkan *downtime* dan mengganggu aktivitas operasional, terutama pada divisi yang sangat bergantung pada koneksi internet.

4. Tidak Adanya Sistem *Monitoring* Jaringan. Saat ini, perusahaan belum menggunakan sistem *monitoring* jaringan seperti The Dude, *Zabbix*, atau sejenisnya. Hal ini menyulitkan tim IT dalam memantau kondisi jaringan secara *real-time*, mendeteksi gangguan lebih awal, serta menganalisis penggunaan *bandwidth* dan performa perangkat jaringan.

5. Minimnya Dokumentasi dan Standar Operasional Prosedur (SOP).

Dokumentasi jaringan seperti topologi, konfigurasi perangkat, dan alokasi *IP address* belum terdokumentasi dengan baik. Selain itu, belum tersedia SOP yang mengatur penanganan gangguan jaringan, proses *backup*, dan pemeliharaan sistem secara berkala.

6. Keamanan Jaringan Masih Dasar. Sistem keamanan jaringan masih terbatas pada konfigurasi *firewall* dasar dari Mikrotik. Belum diterapkan

segmentasi jaringan (VLAN), *autentikasi* pengguna terpusat, atau sistem deteksi dan pencegahan intrusi (IDS/IPS). Hal ini meningkatkan risiko terhadap serangan dari luar maupun kesalahan internal.

Permasalahan-permasalahan tersebut menunjukkan bahwa jaringan yang berjalan saat ini belum memenuhi standar efisiensi dan keandalan yang dibutuhkan oleh perusahaan. Oleh karena itu, diperlukan solusi yang tepat dan terukur untuk meningkatkan performa jaringan, salah satunya melalui implementasi metode *load balancing* dan *failover* berbasis Mikrotik.

3.4. Alternatif Pemecahan Masalah

Guna mengatasi permasalahan yang teridentifikasi pada jaringan komputer PT. ABB Sakti Industri, diperlukan penerapan solusi yang tepat dan terukur agar kinerja jaringan meningkat, waktu henti diminimalkan, serta keamanan jaringan lebih terjamin. Adapun *alternatif* solusi yang diusulkan adalah sebagai berikut:

1. Implementasi *load balancing* dilakukan dengan memanfaatkan fitur PCC (*Per Connection Classifier*) pada *router* Mikrotik. Melalui konfigurasi ini, distribusi trafik internet dapat diatur agar terbagi secara proporsional ke dua jalur ISP berdasarkan karakteristik koneksi atau protokol. Hal ini akan mengoptimalkan pemanfaatan *bandwidth* dari kedua ISP dan mengurangi beban pada satu jalur koneksi.
2. Penerapan *Failover* Otomatis. Untuk menghindari *downtime* saat ISP utama mengalami gangguan, *failover* otomatis dapat dikonfigurasi menggunakan fitur *Netwatch* atau *script routing* pada Mikrotik. Sistem ini akan secara otomatis

mendeteksi koneksi yang terputus dan mengalihkan *trafik* ke jalur ISP cadangan tanpa intervensi manual dari tim IT.

3. Penerapan sistem *monitoring* jaringan dilakukan dengan memanfaatkan perangkat lunak seperti *The Dude*, *Zabbix*, atau *Cacti* untuk memantau kondisi jaringan secara *real-time*. Dengan sistem ini, tim IT dapat mengetahui status perangkat, penggunaan *bandwidth*, dan mendeteksi gangguan lebih awal sehingga penanganan dapat dilakukan lebih cepat dan efisien.
4. Pembuatan Dokumentasi dan SOP Jaringan. Dokumentasi jaringan yang mencakup topologi, konfigurasi perangkat, alokasi IP *address*, dan prosedur penanganan gangguan perlu disusun secara sistematis. Selain itu, SOP untuk pemeliharaan jaringan, *backup* data, dan penanganan insiden harus dibuat agar proses operasional lebih terstruktur dan dapat dipertanggungjawabkan.
5. Peningkatan Keamanan Jaringan. Untuk meningkatkan keamanan, dapat diterapkan segmentasi jaringan menggunakan VLAN, *autentikasi* pengguna berbasis server (misalnya RADIUS), serta konfigurasi *firewall* yang lebih ketat. Jika memungkinkan, sistem IDS/IPS juga dapat ditambahkan untuk mendeteksi dan mencegah serangan dari luar.
6. Pelatihan dan Pengembangan Tim IT. Agar solusi yang diterapkan dapat berjalan optimal, tim IT perlu diberikan pelatihan terkait konfigurasi Mikrotik, manajemen jaringan, dan penggunaan *tools monitoring*. Hal ini akan meningkatkan kompetensi teknis dan kesiapan dalam menghadapi tantangan jaringan di masa depan.

Dengan menerapkan alternatif solusi di atas, diharapkan jaringan komputer PT. ABB Sakti Industri dapat beroperasi dengan lebih stabil, efisien, dan aman, serta mampu mendukung kebutuhan bisnis perusahaan secara berkelanjutan