

## LOAD BALANCING DENGAN METODE HSRP UNTUK MENINGKATKAN AKSES LAYANAN SERVER PT. TELEKOMUNIKASI INDONESIA TBK.

Muhammad Syafrizal<sup>1)</sup>, Fahrizal<sup>2)</sup>, Omar Pahlevi<sup>3)</sup>

<sup>1)</sup>Prodi Teknologi Komputer, Fakultas Teknik & Informatika, Univ. Bina Sarana Informatika

<sup>2,3)</sup>Prodi Sistem Informasi, Fakultas Teknik & Informatika, Univ. Bina Sarana Informatika

Correspondence author: Fahrizal, fahrizal.fzl@bsi.ac.id, Jakarta, Indonesia

### Abstract

Management of information technology (IT) services in every organization becomes very important nowadays. Matching service availability with company needs is a basic value in determining the performance of the IT department. Making risk-based planning is a way to get a priority scale in determining corrective actions to be taken. By identifying risks, registering risks, and assessing risks that cause network service disruption based on the frequency of risk events and the severity/loss level if the risk occurs, a program plan is obtained to follow up (Risk treatment plan). Problems with network availability such as disconnection, unable to access servers, and busy servers due to overloaded access are problems that occur in the internal network of PT. Telekomunikasi Indonesia Tbk. By implementing a load balancing configuration using the HSRP method, you can add network backups to the internet and servers thereby increasing the availability of access services to servers and the internet when the network is busy and when an incident occurs when one of the networks is disconnected. To increase the capacity of the database server service, a switch port mirroring configuration is implemented as a database backup.

**Keywords:** risk management, HSRP, load balancing

### Abstrak

Manajemen layanan teknologi informasi (TI) dalam setiap organisasi menjadi sangat penting saat ini. Menyesuaikan ketersediaan layanan dengan kebutuhan perusahaan menjadi nilai dasar dalam menentukan kinerja departemen TI. Membuat perencanaan berbasis risiko (*Risk Base Thinking*) merupakan cara untuk mendapatkan skala prioritas dalam menentukan tindakan perbaikan yang akan diambil. Dengan mengidentifikasi risiko, meregistrasi risiko, menilai/assess risiko yang menyebabkan gangguan layanan jaringan berdasarkan frekuensi kejadian risiko dan tingkat keparahan/ kerugian jika risiko itu terjadi, didapatkan rencana program untuk menindak lanjuti (*Risk treatment plan*). Permasalahan ketersediaan jaringan seperti terputusnya koneksi, tidak dapat akses ke server dan server sibuk akibat kelebihan beban akses merupakan permasalahan yang terjadi di jaringan internal kantor PT. Telekomunikasi Indonesia Tbk. Dengan menerapkan konfigurasi *load balancing* menggunakan metode HSRP dapat menambahkan backup jaringan ke internet dan server sehingga meningkatkan ketersediaan layanan akses ke server dan internet pada saat jaringan sibuk dan saat terjadi insiden terputusnya salah satu jaringan. Untuk meningkatkan kapasitas

layanan server basis data diterapkan konfigurasi switch port mirroring sebagai backup basis data.

**Kata Kunci:** manajemen resiko, HSRP, load balancing

## A. PENDAHULUAN

Perkembangan teknologi informasi menimbulkan dampak yang sangat masif terhadap aktivitas berbisnis dan berorganisasi. Ketergantungan terhadap ketersediaan layanan teknologi informasi menjadi tidak bisa dihindarkan lagi. Tuntutan terhadap kinerja yang baik sesuai kebutuhan dan kesepakatan antara departemen teknologi informasi (TI) dengan *stakeholder* nya, menjadikan tim departemen TI harus berbenah diri dengan menerapkan tata kelola yang baik sesuai dengan panduan standar praktek terbaik (*Best Practice*) diantaranya *IT Service Management System* yang dikeluarkan bersama-sama antara *International Organization for Standardization (IOS)* yang lebih dikenal dengan ISO dan *International Electronical Commission (IEC)* yaitu ISO/IEC 20000-1:2018 (Yoewono & Prasetyo, 2022). Pada penerapannya standar tersebut menekankan perencanaan manajemen layanan berbasis risiko / *risk base thinking* (Susilo & Kaho, 2018). Dengan perencanaan manajemen layanan berbasis risiko tersebut penulis mencoba membuat solusi dari permasalahan yang terjadi di PT. Telekomunikasi Indonesia Tbk, lebih tepatnya pada kantor Direktorat Digital Business (DDB).

Pada jaringan perusahaan terdapat permasalahan yang menyebabkan kinerja layanan yang diberikan departemen IT kepada organisasi menjadi terhambat. Keluhan dari pengguna jaringan terkait kinerja jaringan dan server yang lambat, terganggunya proses bisnis organisasi akibat problem atau *maintenance* jaringan dan *maintenance* server masih terjadi.

Permasalahan tersebut dibahas melalui penelitian manajemen risiko hingga

didapatkan solusi yang tepat beserta dengan teknis konfigurasi jaringan yang diusulkan.

## B. METODE PENELITIAN

Metode yang digunakan untuk mendapatkan informasi yang dibutuhkan dalam penelitian ini yaitu dengan metode

1. Wawancara dengan departemen Teknologi Informasi (TI).

Wawancara dilakukan untuk mendapatkan informasi terkait spesifikasi layanan jaringan yang ada di perusahaan baik *hardware* maupun *software*, termasuk topologi jaringan yang telah diterapkan.

Wawancara juga dilakukan untuk memperoleh permasalahan yang ada yang menjadi risiko layanan jaringan, frekuensi kejadian risiko dan dampak dan kerugian yang ditimbulkan saat risiko terjadi.

2. Observasi langsung.

Observasi langsung dilakukan untuk mendapatkan informasi terkait permasalahan yang spesifik dengan mencoba dan mengamati kejadian risiko. Observasi juga dilakukan untuk mencari sebab timbulnya risiko (*root cause analysis*).

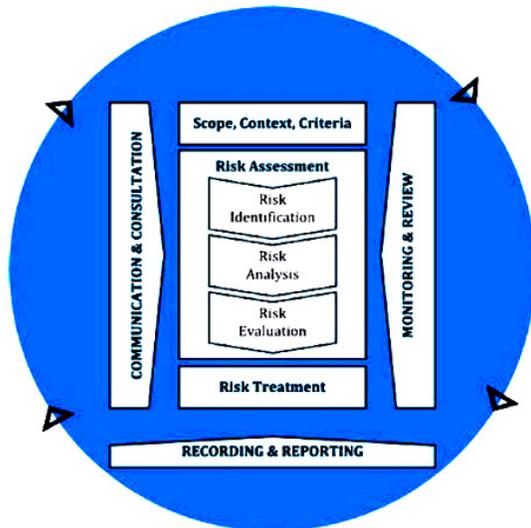
3. Menggunakan metode proses manajemen risiko.

Metode ini digunakan untuk mengelola risiko yang ada pada sistem informasi dan jaringan perusahaan. Metode ini terdiri atas:

a. Mengidentifikasi risiko

b. Menilai risiko berdasarkan frekuensi kejadian risiko (*probability*) dan tingkat keparahan atau dampak (*impact*) jika risiko itu benar-benar terjadi dalam penelitian ini digunakan risk assessment matriks.

- c. Melakukan *root cause analysis* untuk mencari penyebab mengapa risiko itu terjadi
- d. Membuat program mitigasi risiko untuk menangani risiko agar risiko-risiko tersebut tidak terjadi di kemudian hari.



Gambar 1. Kerangka kerja proses manajemen risiko.

untuk melakukan penilaian/ assessment risiko digunakan tabel probabilitas dan impact.

4. Studi pustaka  
Metode ini digunakan untuk mencari informasi penelitian terkait yang telah ada melalui jurnal-jurnal terkait, buku-buku dan artikel di internet. Metode ini juga digunakan untuk mencari solusi konfigurasi jaringan yang bisa diusulkan.
5. Menggunakan metode penelitian laboratorium  
Metode ini digunakan untuk mencari konfigurasi jaringan usulan yang tepat sebagai solusi menangani risiko. Metode ini dilakukan dengan menggunakan simulator jaringan packet tracer. Metode ini juga dilakukan untuk menguji konfigurasi jaringan usulan.

Sebagai referensi penelitian ini penulis mengambil dari beberapa penelitian terdahulu antara lain:

1. Paper yang berjudul “*Manual Load Balancing pada Redundancy Link Menggunakan Multi-Group Hot Standby Router Protocol*”. Dalam jurnal tersebut disebutkan disebutkan HSRP merupakan salah satu metode yang dapat digunakan dalam membangun redundancy link untuk jaringan layer 3, walaupun HSRP tidak memiliki fitur load balancing namun dalam implementasinya pada 4 VLAN didapatkan hasil transisi penanganan *failover* dan transisi berjalan lancar dan jarang terjadi kehilangan paket atau *time out*, namun terjadi peningkatan *delay* beberapa saat sebelum akhirnya kembali normal. Selain itu, ditemukan bahwa terdapat perbedaan yang signifikan antara waktu *failover* dan waktu pemulihan yang diperlukan ketika ada masalah jaringan pada satu antarmuka fisik dan antarmuka dengan empat sub-antarmuka yang mewakili empat grup HSRP untuk setiap VLAN. Dimana penanganan *failover* antara keduanya memiliki selisih waktu 6,35 detik, sedangkan waktu *recovery* memiliki selisih waktu 6,58 detik (Hariadi, 2021).
2. Paper yang berjudul “*Analisis IT Risk Management di Universitas Bina Darma Menggunakan ISO 31000*” yang ditulis oleh Yeni Erlika, Muhammad Izman Herdiansyah dan A. Haidar Mirza. Dalam jurnal tersebut dijelaskan tentang perlunya evaluasi dalam penerapan manajemen IT untuk mengukur penanganan risiko yang terjadi. pada penelitian tersebut bertujuan untuk menganalisis dan mengetahui proses manajemen risiko IT yang diadopsi di Universitas Bina Darma Palembang menggunakan pendekatan ISO 31000, dan berfokus pada evaluasi praktik manajemen IT yang mencakup tiga tahapan; identifikasi, analisis, dan

- perlakuan risiko. dan pada penelitian tersebut menghasilkan laporan risiko TI pada aplikasi sistem (Erlika et al., 2020).
- Paper yang berjudul “Pengukuran Tingkat Layanan Teknologi Informasi pada PT XYZ menggunakan Framework IT Service Management”. Pada penelitian ini disebutkan untuk mewujudkan tata kelola TI yang baik, audit TI perlu dilakukan supaya ada perbaikan terkait teknologi informasi yang memadai. Penelitian tersebut mengukur bagaimana implementasi *framework* ISO 20000-1: 2011 untuk mengukur tingkat layanan teknologi informasi di PT.XYZ. Penelitian tersebut memiliki 2 tujuan utama yaitu supaya dapat memahami proses implementasi *framework* ISO 20000-1: 2011 untuk mengukur tingkat layanan teknologi informasi pada PT.XYZ dan sebagai upaya perbaikan berkelanjutan dengan rekomendasi yang tepat untuk meningkatkan tingkat layanan teknologi informasi pada PT.XYZ (Millah et al., 2018).

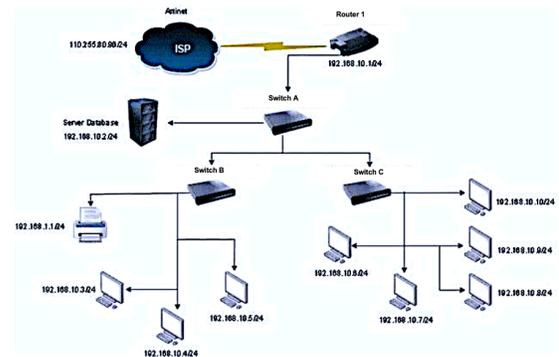
### C. HASIL DAN PEMBAHASAN

#### Spesifikasi layanan

Adapun ruang lingkup layanan yang akan diteliti yaitu meliputi jaringan internal kantor Direktorat Digital Bussiness (DDB). Dari jaringan internal karyawan dan dari internet terdapat kebutuhan mengakses ke server web perusahaan. web server tersebut memiliki akses ke server basis data. Layanan yang dibutuhkan dalam proses bisnis perusahaan mensyaratkan bahwa server tersebut harus dapat diakses 24 jam sehari 7 hari seminggu. namun diizinkan untuk maintenance berkala pada hari-hari libur sabtu atau minggu pada pekan kedua setiap bulan. sebagai kebijakan perusahaan menetapkan kejadian risiko gangguan tidak boleh mengganggu *service level agreement* (SLA) layanan sebesar 90%.

#### Konfigurasi Jaringan

Untuk menganalisa sumber risiko terkait koneksi jaringan, didapatkan melalui skema jaringan seperti gambar 2.



Sumber: TELKOM DDB (PT Telekomunikasi Indonesia Tbk)

Gambar 2. Skema Jaringan

Berdasarkan skema jaringan terdapat sumber risiko kegagalan jaringan sangat tergantung dengan kinerja router dan switch utama. Berdasarkan laporan insiden layanan jaringan terdapat keluhan diantaranya :

- Jaringan yang lambat terutama saat waktu sibuk yaitu ketika banyak yang mulai login jaringan.
- terganggunya pekerjaan saat maintenance server web.
- kinerja web *server* yang lambat terutama saat banyak user yang login
- Akses internet yang lambat terutama saat jam sibuk
- jika router error maka seluruh jaringan tidak dapat konek ke internet.
- kehilangan data saat transaksi server database *down*.

Pada penelitian ini hanya risiko yang bersifat mayor saja yang ditampilkan sebagai fokus masalah pada penelitian ini. Berdasarkan insiden tersebut dibuat tabel skala penilaian risiko berdasarkan tingkat frekuensi insiden terjadi menggunakan skala penilaian dalam tahun dan tingkat keparahan jika risiko/insiden itu terjadi berdasarkan kehilangan ketersediaan layanan berdasarkan jumlah durasi *downtime*.

Tabel 1. Tabel Skala Penilaian Risiko

| Frekuensi dalam satu tahun | Nilai Probabilitas | Down time      | Nilai Dampak |
|----------------------------|--------------------|----------------|--------------|
| 1- 10 kali                 | 1                  | 1-3 jam        | 1            |
| 11 - 20 kali               | 2                  | 4-8 jam        | 2            |
| 21 - 30 kali               | 3                  | 9 jam – 1 hari | 3            |
| > 30 kali                  | 4                  | >1 hari        | 4            |

berdasarkan tabel skala penilaian risiko didapatkan

Tabel 2. Tabel Penilaian Risiko

| No | Layanan/ Proses                 | Aset                    | Deskripsi Risiko                        | Nilai Prob | Nilai Dampak | Nilai Risiko Dasar |
|----|---------------------------------|-------------------------|---|------------|--------------|--------------------|
| 1  | koneksi jaringan ke server      | Router 1                | Hilangnya koneksi jaringan ke server    | 4          | 4            | 8                  |
| 2  | koneksi jaringan ke internet    | Router 1                | Hilangnya koneksi jaringan ke internet  | 4          | 4            | 8                  |
| 3  | ketersediaan layanan server web | Server                  | hilangnya availabilitas server web      | 3          | 4            | 7                  |
| 4  | koneksi jaringan internal       | Koneksi Switch & Router | terputusnya koneksi jaringan inter VLAN | 2          | 4            | 6                  |
| 5  | Layanan Database Server         | Server                  | kehilangan data akibat DB server down   | 1          | 4            | 5                  |

Berdasarkan hasil wawancara dengan pihak terkait dampak risiko yang paling harus dihindari adalah risiko kehilangan data dan ketersediaan koneksi ke server. Berdasarkan penilaian risiko tersebut didapatkan urutan prioritas risiko sebagai berikut

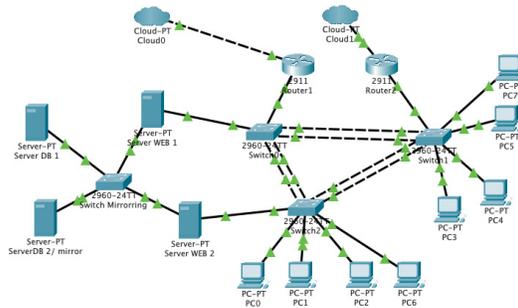
1. Kehilangan data akibat DB server down
2. Hilangnya Koneksi Jaringan ke Server
3. Hilangnya koneksi jaringan ke internet
4. hilangnya availabilitas server web
5. Terputusnya koneksi jaringan inter VLAN

Berdasarkan *Root Cause Analysis* (RCA) didapatkan tabel sebagai berikut:

Tabel 3. Prioritas risiko dan Root Cause Analysis (RCA)

| No | Layanan/ Proses                        | Aset terdampak              | Penyebab  | Rekomendasi Solusi  |
|----|--|-----------------------------|---|---|
| 1  | Kehilangan data akibat DB Server Down  | Server DB                   | Server DB Down terdapat data yang tidak terbackup karena backup belum dilakukan secara realtime | Membangun konfigurasi backup realtime (dengan mirroring server)           |
| 2  | Hilangnya koneksi jaringan ke server   | Router 1 & Server WEB       | Router Kelebihan beban jaringan, dan tidak ada backup Web server                                | membangun redundancy router dan web server (HSRP & redundancy server web) |
| 3  | Hilangnya koneksi jaringan ke internet | Router 1                    | router kelebihan beban  | membangun redundancy router (HSRP)  |
| 4  | Hilangnya availabilitas server web     | Router 1 & Web Server       | kelebihan beban server web  | membangun redundancy web server   |
| 5  | Hilangnya koneksi jaringan inter VLAN  | Koneksi Switch dan Router 1 | hanya mengandalkan satu link switch antar divisi  | membangun jaringan redundancy link (STP)                                  |

Berdasarkan tabel *root cause analysis* dan rekomendasi solusi diatas dirancang jaringan usulan seperti jaringan di bawah ini



Gambar 3. Topologi jaringan Usulan

Pada konfigurasi *topologi* jaringan yang diusulkan merupakan solusi untuk mengurangi risiko namun demikian masih terdapat risiko yang mungkin terjadi (*residual Risk*)

1. Untuk mengurangi risiko nomor 1  
 Kehilangan data akibat DB server *down* dapat ditekan risikonya dengan cara backup realtime dengan metode mirroring server. pada gambar 3 diwakilkan dengan switch mirroring, namun untuk lebih mengurangi lagi risiko kehilangan data penulis merekomendasikan agar perusahaan membangun *sistem disaster recovery plan (DRP)* yang berbasis *cloud*. agar risiko kehilangan data karena bencana infrastruktur backup yang masih satu lokasi dapat dikurangi.
2. Untuk mengurangi risiko 2, 3 dan 5  
 Yaitu hilangnya koneksi jaringan ke *server*, hal tersebut disebabkan oleh *router* yang kelebihan beban jaringan sehingga akses ke server dari jaringan internal tidak stabil.  
 Untuk mengurangi risiko tersebut penulis merekomendasikan agar perusahaan membangun *redundancy router* misalnya dengan menerapkan *Hot standby routing protocol (HSRP)* sebagai tambahan penulis juga merekomendasikan *redundancy link* pada jaringan perusahaan untuk meningkatkan imunitas terhadap risiko terputusnya sebagian maupun keseluruhan jaringan

seperti menerapkan *Spanning tree protocol (STP)*.

3. Untuk mengurangi risiko nomor 4.  
 yaitu hilangnya *availability server web*, penulis merekomendasikan agar perusahaan membangun *redundancy server web* dengan menerapkan *clustering* pada server.

### Hasil Pengujian

1. Pengujian konfigurasi *switch STP*  
 Pengujian konfigurasi jaringan STP dilakukan dengan metode *failover* yaitu dengan memutus koneksi atau menonaktifkan salah satu switch salah satu dari tiga switch didapatkan hanya perangkat yang *switch*nya di non aktifkan yang terdampak keseluruhan jaringan masih dapat terkoneksi. jika yang dilakukan pemutusan salah satu link antar *switch*, tidak ada perangkat yang terdampak, semua koneksi jaringan masih dapat dilakukan.
2. Pengujian pada konfigurasi HSRP  
 Pengujian konfigurasi jaringan HSRP dilakukan dengan metode *failover* yaitu dengan menonaktifkan salah satu router. Didapatkan hasil semua jaringan masih dapat terkoneksi dengan baik walaupun beberapa komputer mengalami gangguan selama 30 detik namun akhirnya dapat terkoneksi dengan baik.
3. Pengujian pada *Redundancy Server*  
 Pengujian konfigurasi *redundancy server* dilakukan dengan metode *failover* yaitu dengan menonaktifkan salah satu server secara bergantian. Didapatkan hasil semua jaringan masih dapat terkoneksi dengan baik walaupun beberapa komputer mengalami gangguan koneksi ke server selama 30 detik namun akhirnya dapat mengakses server web kembali. durasi tersebut dapat dikurangi dengan cara mengakses IP address server web yang masih aktif secara langsung

#### D. PENUTUP

Hasil dari penelitian ini didapatkan bahwa sistem manajemen layanan berbasis risiko dapat diterapkan untuk menyelesaikan permasalahan IT perusahaan. dengan mengidentifikasi risiko yang ada kemudian menilai risiko-risiko tersebut untuk dibuat skala prioritas untuk menentukan risiko-risiko mana yang menjadi prioritas harus dilakukan perbaikan melalui program-program mitigasi risiko.

Meningkatkan availability jaringan dapat dibangun dengan menerapkan konfigurasi *redundancy router* dengan HSRP, *redundancy link* dengan menerapkan STP dan *redundancy server* dengan menerapkan konfigurasi *clustering*.

Meningkatkan availabilitas dan integritas data pada *database* dapat diterapkan dengan membangun *real time backup* server dengan menerapkan *mirroring server*.

Konfigurasi-konfigurasi yang diterapkan dalam penelitian ini masih dapat ditingkatkan dengan menggunakan metode yang lain, misalnya untuk meningkatkan availability server web dan database, perusahaan dapat mengalihdayakan infrastrukturnya dengan memanfaatkan layanan cloud pada data center apabila risiko-risiko yang mungkin timbul dari pengalihdayaan tersebut telah diidentifikasi dan dinilai serta diantisipasi dengan baik.

Risiko-risiko yang diidentifikasi dalam penelitian ini belum mencakup aspek keamanan informasi dari sisi *confidentiality* dan *integrity* dan masih perlu dilakukan penelitian lebih lanjut.

#### Ucapan Terima Kasih

Sebagai ungkapan rasa hormat penulis mengucapkan terimakasih kepada manajemen Direktorat Digital Business (DDB) PT. Telekomunikasi Indonesia Tbk. Serta Bapak Irfan Permadi selaku Mentor selama penelitian ini.

#### E. DAFTAR PUSTAKA

- Erlika, Y., Herdiansyah, M. I., & Mirza, A. H. (2020). Analisis IT Risk Management di Universitas Bina Darma Menggunakan ISO31000. *Jurnal Ilmiah Informatika Global*, 11(1), 55–62. <https://doi.org/10.36982/jig.v11i1.1073>
- Hariadi, F. (2021). Manual Load Balancing pada Redundancy Link Menggunakan Multi-Group Hot Standby Router Protocol. *Jurnal Teknik Informatika Dan Sistem Informasi*, 7(1), 206–217. <https://doi.org/10.28932/jutisi.v7i1.3403>
- Millah, A., Rozas, I. S., & Amrozi, Y. (2018). Pengukuran Tingkat Layanan Teknologi Informasi Pada PT. XYZ Menggunakan Framework IT Services Management. *Prosiding SNST Ke-9 Tahun 2018*, 226–231.
- Susilo, L. J., & Kaho, V. R. (2018). *Manajemen Risiko Berbasis ISO 31000:2018: Panduan Untuk Risk Leaders dan Risk Practitioners*. Jakarta : PT. Grasindo.
- Yoewono, J. O., & Prasetyo, A. H. (2022). Rancangan Dan Proses Manajemen Risiko Pada PT Surya Selaras Cita. *Jurnal Muara Ilmu Ekonomi Dan Bisnis*, 6(1), 56. <https://doi.org/10.24912/jmieb.v6i1.12207>