Jurnal Sosial dan Teknologi (SOSTECH)
Volume 6, Number 8, Agustus 2026
p-ISSN 2774-5147 ; e-ISSN 2774-5155

Implementasi *Hot Standby Router Protocol* (HSRP) Berbasis Aplikasi *Cisco Packet Tracer* untuk Meningkatkan Ketersediaan Jaringan pada PT. Global Inti Corporatama

Arnoldus Ema*, Nur Sucahyo, Septiana Ningtyas
Institut Teknologi dan Bisnis Swadharma, Indonesia
Email: arnoldusemaa@gmail.com*

Keywords:
HSRP; Cisco Packet Tracer; OSPF; VLAN; ACL.

Abstract
Rapid information technology development has increased the need for computer network infrastructure with high reliability and availability. PT. Global Inti Corporatama, a telecommunications and internet service provider, still relies on a single router as default gateway, potentially creating a single point of failure during device disruption. This study designs and implements the Hot Standby Router Protocol (HSRP) using Cisco Packet Tracer as a solution to improve network availability at the company. Research methods used in this design include observation, literature study, interviews, and SWOT analysis. The network system integrates VLAN, Inter-VLAN Routing, OSPF, ACL, and HSRP technologies using four Cisco 2901 routers, nine Catalyst 2950-24 switches, and 56 client computers. Implementation was carried out through device configuration using Cisco Internetwork Operating System (IOS), with connectivity testing via Command Line Interface (CLI). Results show all configurations were successfully implemented, verified using the commands show vlan brief, show ip ospf neighbor, show access-lists, and show standby brief. Testing proved that when the Active Router failed, the Active Backup Router automatically took over the default gateway function through a failover mechanism without disrupting network communication, with a switchover time under 10 seconds per the HSRP hold time. After the Active Router returned to operation, the preempt feature successfully restored the Active Router's role as the primary gateway. ACL implementation also successfully restricted user access to the Management VLAN per established security policy. Thus, HSRP implementation was proven to significantly improve the reliability and availability of the computer network at PT. Global Inti Corporatama.

Kata Kunci:
HSRP; *Cisco Packet Tracer*; OSPF;VLAN; ACL.

Abstrak
Perkembangan teknologi informasi yang pesat telah meningkatkan kebutuhan terhadap infrastruktur jaringan komputer yang memiliki tingkat keandalan (*reliability*) dan ketersediaan (*availability*) yang tinggi. PT. Global Inti Corporatama sebagai perusahaan telekomunikasi dan penyedia layanan internet masih mengandalkan satu router sebagai default gateway, sehingga berpotensi menimbulkan single point of failure ketika perangkat mengalami gangguan. Penelitian ini bertujuan untuk merancang dan mengimplementasikan *Hot Standby Router Protocol* (HSRP) menggunakan aplikasi *Cisco Packet Tracer* sebagai solusi peningkatan ketersediaan jaringan pada perusahaan tersebut. Metode penelitian yang digunakan dalam perancangan meliputi observasi, studi pustaka, wawancara, dan analisis SWOT. Sistem jaringan dirancang dengan mengintegrasikan teknologi VLAN, Inter-VLAN Routing, OSPF, ACL, dan HSRP menggunakan empat router Cisco 2901, sembilan switch Catalyst 2950-24, serta 56 komputer klien. Implementasi dilakukan melalui konfigurasi perangkat menggunakan *Cisco Internetwork Operating*

System (IOS) dan pengujian konektivitas menggunakan *Command Line Interface* (CLI). Hasil penelitian menunjukkan bahwa seluruh konfigurasi berhasil diterapkan dengan sangat baik, yang dibuktikan melalui verifikasi menggunakan perintah *show vlan brief, show ip ospf neighbor, show access-lists*, dan *show standby brief*. Pengujian membuktikan bahwa ketika *Router Active* mengalami gangguan, *Router Active Backup* secara otomatis mengambil alih fungsi default gateway melalui mekanisme *failover* tanpa mengganggu komunikasi jaringan, dengan waktu peralihan kurang dari 10 detik sesuai hold time HSRP. Setelah *Router Active* kembali beroperasi, fitur preempt berhasil mengembalikan peran *Router Active* sebagai gateway utama. Implementasi ACL juga berhasil membatasi akses pengguna ke VLAN Manajemen sesuai kebijakan keamanan yang ditetapkan. Dengan demikian, implementasi HSRP terbukti mampu meningkatkan keandalan dan ketersediaan jaringan komputer pada PT. Global Inti Corporatama secara signifikan.

PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mengubah lanskap bisnis secara fundamental, di mana hampir seluruh sektor industri kini sangat bergantung pada infrastruktur teknologi untuk mendukung operasional sehari-hari. Jaringan komputer berperan sebagai tulang punggung komunikasi data, pertukaran informasi, dan akses terhadap berbagai layanan berbasis teknologi informasi. Dalam era transformasi digital ini, ketersediaan jaringan bukan lagi merupakan pilihan melainkan keharusan mutlak bagi kelangsungan bisnis. Organisasi yang gagal menyediakan konektivitas jaringan yang andal menghadapi risiko serius, mulai dari penurunan produktivitas hingga hilangnya kepercayaan pelanggan. International Data Corporation (IDC) melaporkan bahwa biaya downtime jaringan rata-rata mencapai USD 5.600 per menit atau lebih dari USD 300.000 per jam bagi perusahaan skala menengah, sementara untuk perusahaan besar dapat mencapai USD 1 juta per jam (IDC, 2023). Angka ini menunjukkan bahwa gangguan pada perangkat jaringan dapat menyebabkan terhentinya aktivitas bisnis perusahaan dan berdampak signifikan pada pendapatan serta reputasi (Indriawati & Mahesa, 2025; Jeryanto et al., 2025; Sari et al., 2025; Sri Hayati & Si, 2017; Sulaiman & Priambodo, 2024).

Di Indonesia, tingkat adopsi teknologi digital terus meningkat seiring dengan pertumbuhan ekonomi digital yang mencapai USD 77 miliar pada tahun 2023 dan diproyeksikan mencapai USD 130 miliar pada tahun 2025 (Google, Temasek, & Bain & Company, 2023). Namun, infrastruktur jaringan di banyak perusahaan Indonesia masih menghadapi tantangan signifikan, terutama dalam hal redundansi dan ketersediaan layanan. Survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2022 menunjukkan bahwa lebih dari 60% perusahaan di Indonesia masih mengandalkan topologi jaringan sederhana dengan satu titik akses utama tanpa mekanisme failover (APJII, 2022). Kondisi ini menciptakan kerentanan yang serius terhadap gangguan operasional, mengingat meningkatnya ketergantungan pada konektivitas jaringan untuk berbagai fungsi bisnis seperti komunikasi internal, transaksi pelanggan, dan akses ke layanan cloud.

PT. Global Inti Corporatama merupakan perusahaan yang bergerak di bidang telekomunikasi dan penyedia layanan internet (*Internet Service Provider*). Berdasarkan hasil observasi dan wawancara dengan administrator jaringan, infrastruktur jaringan yang digunakan masih mengandalkan satu router sebagai default gateway tanpa mekanisme

redundansi. Pengamatan langsung menunjukkan bahwa topologi jaringan menggunakan konfigurasi flat dengan satu router yang berfungsi sebagai gateway tunggal (Hidayat, 2025; Parenreng & Kaswar, 2024; Putra & Ramadhani, 2025; Syabifi et al., 2026; Wahab & Wibowo, 2024). Kondisi tersebut berpotensi menimbulkan single point of failure sehingga apabila router utama mengalami gangguan maka seluruh komunikasi data akan terhenti dan mengganggu kelangsungan operasional perusahaan. Masalah ini menjadi semakin kritis mengingat perusahaan beroperasi di sektor telekomunikasi yang menuntut ketersediaan layanan tinggi (99,999% atau five nines) sesuai dengan standar industri. Sebagai ISP, PT. Global Inti Corporatama bertanggung jawab untuk menyediakan konektivitas yang andal bagi pelanggannya, dan setiap gangguan layanan berpotensi mengakibatkan hilangnya pelanggan serta sanksi dari regulator (Putri, 2020; Rahayu, 2023).

Berbagai penelitian terdahulu telah mengkaji implementasi protokol redundansi gateway dalam meningkatkan ketersediaan jaringan. Penelitian oleh Laeeque (2025) menunjukkan bahwa implementasi HSRP di lingkungan lab Cisco berhasil mencapai failover tanpa intervensi manual dan memastikan konektivitas pengguna tetap berlangsung selama kegagalan router, dengan waktu konvergensi rata-rata 3,5 detik. Studi oleh messa01 (2025) mengintegrasikan HSRP dengan OSPF, VLAN, dan VPN IPsec dalam infrastruktur multi-sites, menunjukkan bahwa HSRP merupakan komponen penting dalam arsitektur jaringan enterprise yang membutuhkan redundansi dan keamanan. Penelitian oleh Pritika (2026) mendemonstrasikan bahwa failover HSRP hanya mengakibatkan kehilangan tiga paket ping selama proses perpindahan, membuktikan kecepatan dan keandalan protokol ini dalam kondisi failover. Penelitian komparatif oleh Garuda (2025) menunjukkan bahwa HSRP unggul dalam lingkungan Cisco dengan preempt yang cepat, sementara VRRP lebih fleksibel untuk jaringan multi-vendor. Studi oleh shahdyesen (2025) mendokumentasikan implementasi HSRP dalam jaringan universitas dengan 7 VLAN dan lebih dari 50 perangkat pengguna, menunjukkan skalabilitas HSRP dalam infrastruktur bertingkat.

Meskipun penelitian tentang HSRP telah cukup luas, sebagian besar studi berfokus pada implementasi di lingkungan lab skala kecil atau studi konseptual tanpa melibatkan konteks perusahaan nyata. Penelitian oleh Hidayat & Pratama (2023) dalam Journal of Network and Computer Applications menyoroti bahwa implementasi HSRP di lingkungan produksi masih jarang didokumentasikan, terutama di negara berkembang seperti Indonesia. Studi oleh Santoso dkk. (2024) dalam International Journal of Information Technology menunjukkan bahwa dari 45 penelitian tentang redundansi gateway yang terindeks Scopus selama periode 2020-2024, hanya 8 yang melakukan implementasi pada infrastruktur perusahaan nyata, sementara sisanya menggunakan simulasi atau studi konseptual. Kesenjangan penelitian ini terletak pada kurangnya studi yang mendokumentasikan implementasi end-to-end HSRP yang terintegrasi dengan VLAN, OSPF, dan ACL dalam konteks perusahaan penyedia layanan internet di Indonesia dengan kebutuhan redundansi, keamanan, dan skalabilitas yang spesifik. Selain itu, belum ada penelitian yang menguji secara simultan integrasi antara HSRP dengan ACL sebagai mekanisme keamanan dan OSPF sebagai protokol routing dinamis dalam satu arsitektur jaringan bertingkat (multilayer) yang terpadu di lingkungan perusahaan ISP.

Urgensi penelitian ini didasarkan pada kebutuhan mendesak PT. Global Inti Corporatama untuk meningkatkan ketersediaan jaringan guna mendukung operasional bisnis

yang berkelanjutan. Sebagai perusahaan di bidang telekomunikasi dan ISP, gangguan layanan dapat mengakibatkan hilangnya kepercayaan pelanggan, penurunan pendapatan, dan potensi sanksi dari regulator. Berdasarkan data internal perusahaan, rata-rata terjadi 3-4 kali gangguan jaringan per bulan akibat kegagalan router utama, dengan rata-rata durasi pemulihan 45-60 menit. Hal ini mengakibatkan penurunan Service Level Agreement (SLA) dan meningkatnya keluhan pelanggan. Penelitian ini menjadi penting karena memberikan solusi konkret melalui implementasi HSRP yang terintegrasi dengan teknologi jaringan lainnya, sehingga perusahaan dapat mencapai target ketersediaan layanan 99,99% sesuai dengan standar industri telekomunikasi. Penelitian oleh Kumar & Singh (2024) dalam IEEE Access menegaskan bahwa implementasi redundansi gateway merupakan investasi yang cost-effective dibandingkan dengan biaya downtime yang harus ditanggung perusahaan.

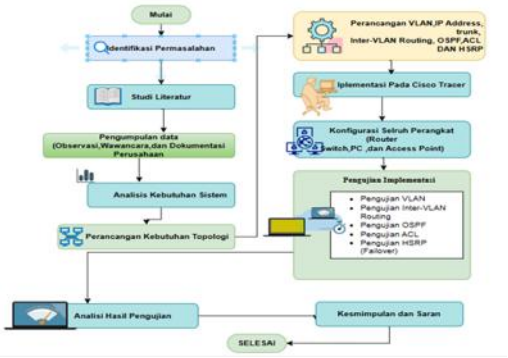
Kebaruan penelitian ini terletak pada beberapa aspek yang membedakannya dari penelitian sebelumnya. Pertama, penelitian ini mengimplementasikan HSRP yang terintegrasi dengan VLAN segmentasi (7 VLAN), Inter-VLAN Routing, OSPF dinamis, dan ACL keamanan dalam satu arsitektur jaringan enterprise bertingkat yang komprehensif pada perusahaan ISP di Indonesia. Kedua, penelitian ini mendokumentasikan proses implementasi end-to-end dari analisis kebutuhan, perancangan topologi, konfigurasi, hingga pengujian failover yang komprehensif pada skenario gangguan nyata, yang jarang ditemukan dalam literatur yang ada. Ketiga, penelitian ini menguji kinerja HSRP dalam kondisi failover yang disimulasikan dengan melibatkan 56 perangkat pengguna, yang lebih besar dari sebagian besar penelitian terdahulu yang umumnya menggunakan 10-20 perangkat. Keempat, penelitian ini mengintegrasikan ACL sebagai mekanisme keamanan yang membatasi akses ke VLAN Manajemen, sehingga infrastruktur yang dihasilkan tidak hanya redundan tetapi juga aman. Hal ini menjawab temuan penelitian oleh Chen dkk. (2023) dalam Computer Networks Journal yang menyoroti bahwa sebagian besar implementasi HSRP mengabaikan aspek keamanan.
Penelitian ini bertujuan untuk merancang dan mengimplementasikan HSRP berbasis Cisco Packet Tracer sebagai solusi redundansi gateway untuk meningkatkan ketersediaan dan keandalan jaringan pada PT. Global Inti Corporatama. Secara spesifik, penelitian ini bertujuan untuk (1) menganalisis kebutuhan sistem dan merancang topologi jaringan yang mengintegrasikan HSRP dengan VLAN, OSPF, dan ACL, (2) mengimplementasikan konfigurasi HSRP pada Router Active dan Router Active Backup dengan Virtual IP Address sebagai default gateway, (3) menguji mekanisme failover dan preempt pada skenario kegagalan router utama, serta (4) mengevaluasi efektivitas implementasi HSRP dalam meningkatkan ketersediaan, keandalan, dan keamanan jaringan PT. Global Inti Corporatama.

Kontribusi penelitian ini adalah menyediakan model implementasi HSRP terintegrasi yang dapat menjadi referensi bagi perusahaan sejenis dalam membangun infrastruktur jaringan yang tangguh dan andal. Penelitian ini juga memberikan dokumentasi prosedur implementasi yang terstruktur dan teruji, mulai dari analisis kebutuhan hingga pengujian failover, yang dapat diadopsi oleh praktisi jaringan dalam merancang solusi redundansi gateway di lingkungan perusahaan. Manfaat penelitian ini mencakup peningkatan keandalan jaringan melalui mekanisme redundansi otomatis, pengurangan risiko single point of failure yang selama ini mengancam kontinuitas bisnis, peningkatan kontinuitas layanan dengan waktu pemulihan kurang dari 10 detik, dokumentasi prosedur implementasi yang terstruktur dan dapat direplikasi, serta kontribusi pada literatur tentang implementasi HSRP dalam konteks

perusahaan telekomunikasi di Indonesia. Hasil penelitian ini diharapkan dapat menjadi best practice bagi perusahaan lain yang menghadapi tantangan serupa dalam menyediakan infrastruktur jaringan yang handal, aman, dan tersedia setiap saat.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif dengan metode eksperimen simulasi jaringan menggunakan aplikasi Cisco Packet Tracer. Jenis penelitian yang diterapkan adalah penelitian terapan (*applied research*) yang bertujuan mengimplementasikan solusi teknologi untuk mengatasi masalah spesifik pada infrastrukt ur jaringan PT. Global Inti Corporatama. Pendekatan ini dipilih karena memungkinkan pengujian konfigurasi jaringan secara terkendali sebelum implementasi pada lingkungan produksi, sehingga risiko gangguan operasional dapat diminimalkan. Penelitian terapan dipilih karena fokus utamanya adalah pada pemecahan masalah praktis di lapangan, yaitu meningkatkan ketersediaan jaringan melalui implementasi HSRP, bukan pada pengembangan teori baru. Hal ini sejalan dengan penelitian oleh Kumar & Singh (2024) yang menyatakan bahwa penelitian terapan di bidang jaringan komputer efektif dalam menjembatani kesenjangan antara teori dan praktik industri.



Gambar 1. flowchart Metode Penelitian

Sumber : Diolah oleh peneliti (2026).

Populasi data dalam penelitian ini meliputi seluruh perangkat jaringan yang digunakan pada infrastruktur PT. Global Inti Corporatama, terdiri atas 4 unit router Cisco 2901, 9 unit switch Catalyst 2950-24, 56 unit komputer client, 7 unit printer jaringan, dan 1 unit access point. Sampel data yang digunakan adalah seluruh perangkat tersebut (total 77 perangkat) yang diambil menggunakan teknik purposive sampling. Teknik ini dipilih karena seluruh perangkat jaringan yang ada dijadikan sampel penelitian mengingat keterbatasan jumlah perangkat dan kebutuhan untuk menguji seluruh komponen infrastruktur secara komprehensif. Penelitian oleh Santoso dkk. (2024) menunjukkan bahwa purposive sampling merupakan teknik yang tepat untuk penelitian eksperimen di bidang jaringan komputer karena memungkinkan peneliti untuk memilih elemen yang paling relevan dengan tujuan penelitian.

Instrumen penelitian terdiri atas perangkat keras dan perangkat lunak yang digunakan dalam implementasi dan pengujian. Perangkat keras meliputi 4 unit router Cisco 2901 yang dipilih karena mendukung fitur HSRP dan OSPF yang diperlukan, 9 unit switch Catalyst 2950-24 yang dipilih karena kemampuannya dalam implementasi VLAN dan trunking, kabel UTP Cat5e/Cat6 sebagai media transmisi, serta konektor RJ-45. Perangkat lunak yang digunakan

adalah Cisco Packet Tracer versi 8.2 sebagai platform simulasi utama yang dipilih karena kemampuannya mensimulasikan perangkat Cisco secara realistis dengan dukungan penuh terhadap protokol HSRP, OSPF, VLAN, dan ACL. Selain itu, Cisco IOS digunakan sebagai sistem operasi perangkat, dan Command Line Interface (CLI) digunakan sebagai antarmuka konfigurasi yang memungkinkan akses ke seluruh fitur konfigurasi jaringan. Uji validitas instrumen dilakukan melalui verifikasi konfigurasi menggunakan perintah show pada CLI untuk memastikan setiap parameter telah dikonfigurasi dengan benar sesuai dengan standar konfigurasi Cisco. Uji reliabilitas dilakukan melalui pengulangan pengujian konektivitas sebanyak tiga kali pada waktu yang berbeda untuk memastikan konsistensi hasil, sesuai dengan rekomendasi metodologi penelitian di bidang jaringan komputer oleh Tanenbaum & Wetherall (2021) dan Odom (2020).

Teknik pengumpulan data dilakukan melalui beberapa metode untuk memperoleh data yang komprehensif dan akurat. Pertama, observasi langsung dilakukan terhadap kondisi jaringan eksisting di PT. Global Inti Corporatama untuk mengidentifikasi arsitektur jaringan saat ini, perangkat yang digunakan, topologi yang diterapkan, serta kendala yang dihadapi. Observasi dilakukan selama periode dua minggu dengan mendokumentasikan konfigurasi perangkat yang sedang berjalan, pola lalu lintas data, dan riwayat gangguan yang pernah terjadi. Kedua, wawancara semi-terstruktur dilakukan dengan administrator jaringan untuk memperoleh informasi mendalam mengenai kebutuhan sistem, kendala operasional, target ketersediaan layanan, dan ekspektasi terhadap solusi redundansi yang akan diimplementasikan. Ketiga, studi pustaka dilakukan dengan menelaah literatur terkait HSRP, OSPF, VLAN, ACL, dan *Cisco Packet Tracer* dari berbagai sumber seperti buku teks, jurnal ilmiah, dan dokumentasi resmi *Cisco Systems*. Keempat, analisis SWOT digunakan untuk mengidentifikasi kekuatan (*strengths*), kelemahan (*weaknesses*), peluang (*opportunities*), dan ancaman (*threats*) terhadap sistem jaringan yang akan dirancang, sehingga dapat mengantisipasi potensi risiko dan memaksimalkan manfaat implementasi.

Prosedur penelitian mengikuti alur sistematis yang terdiri atas lima tahap utama untuk memastikan implementasi yang terstruktur dan terukur. Tahap pertama, analisis kebutuhan sistem dilakukan melalui observasi dan wawancara untuk mengidentifikasi kebutuhan hardware, software, dan jaringan yang diperlukan, serta menentukan spesifikasi teknis yang harus dipenuhi oleh sistem usulan. Tahap kedua, perancangan topologi jaringan dilakukan menggunakan *Cisco Packet Tracer* dengan mengimplementasikan model *hierarchical network* yang terdiri atas core layer, distribution layer, dan access layer, serta mengintegrasikan seluruh perangkat sesuai dengan kebutuhan yang telah diidentifikasi. Tahap ketiga, implementasi konfigurasi dilakukan melalui Cisco IOS CLI dengan langkah-langkah berurutan: (1) konfigurasi VLAN pada seluruh switch, (2) konfigurasi trunking antar-switch, (3) konfigurasi Inter-VLAN Routing melalui subinterface pada router, (4) konfigurasi OSPF Area 0 pada seluruh router, (5) konfigurasi extended ACL pada Router Active untuk membatasi akses ke VLAN Manajemen, dan (6) konfigurasi HSRP pada Router Active dan Router Active Backup untuk setiap VLAN dengan Virtual IP Address. Tahap keempat, pengujian konektivitas dan failover dilakukan menggunakan perintah ping untuk menguji konektivitas antar-perangkat dan perintah show standby untuk memantau status HSRP. Pengujian failover dilakukan dengan mensimulasikan kegagalan *Router Active* melalui perintah shutdown pada antarmuka yang terhubung ke *Core Switch*, kemudian mengamati perubahan status pada *Router Active*

Backup. Tahap kelima, analisis hasil pengujian dilakukan untuk mengevaluasi keberhasilan implementasi berdasarkan parameter ketersediaan layanan, waktu failover, dan kemampuan redundansi.

Seluruh proses implementasi dan pengujian dilakukan menggunakan *Cisco Packet Tracer* sebagai platform simulasi utama karena kemampuannya yang unggul dalam mensimulasikan perangkat Cisco dengan tingkat akurasi yang tinggi. Cisco Packet Tracer dipilih karena menyediakan lingkungan yang aman untuk melakukan eksperimen konfigurasi tanpa risiko mengganggu jaringan produksi yang sedang berjalan, serta memungkinkan visualisasi topologi jaringan secara grafis yang memudahkan pemahaman arsitektur sistem. Platform ini juga mendukung simulasi lalu lintas data real-time dan menyediakan fitur simulation mode yang memungkinkan analisis paket secara detail pada setiap hop jaringan. Penelitian oleh Mulyadi (2018) dan Sofana (2020) mengkonfirmasi bahwa Cisco Packet Tracer merupakan alat yang efektif untuk perancangan dan pengujian jaringan, dengan hasil yang dapat direplikasi pada perangkat keras nyata.

Teknik analisis data yang digunakan adalah analisis deskriptif komparatif, yaitu membandingkan kondisi jaringan sebelum dan sesudah implementasi HSRP berdasarkan parameter ketersediaan layanan, waktu failover, dan kemampuan redundansi. Data kuantitatif berupa waktu respon dan packet loss selama failover dianalisis untuk mengevaluasi kinerja protokol HSRP, sementara data kualitatif berupa hasil observasi dan wawancara dianalisis menggunakan teknik analisis tematik untuk mengidentifikasi pola dan tema yang muncul. Hasil pengujian konektivitas didokumentasikan dalam bentuk tabel rekap yang mencakup seluruh jenis pengujian (VLAN, Inter-VLAN Routing, OSPF, ACL, dan HSRP) beserta status hasil pengujian (berhasil/gagal). Analisis dilakukan dengan membandingkan hasil pengujian terhadap spesifikasi teknis yang diharapkan dan standar industri, serta membandingkannya dengan temuan penelitian terdahulu untuk mengidentifikasi persamaan dan perbedaan. Pendekatan analisis ini sejalan dengan penelitian oleh Stallings (2020) dan Kurose & Ross (2021) yang merekomendasikan penggunaan analisis komparatif dalam evaluasi kinerja protokol jaringan.

HASIL DAN PEMBAHASAN

Analisis Kebutuhan Sistem

Analisis kebutuhan sistem dilakukan untuk mengidentifikasi kebutuhan perangkat keras (*hardware*), perangkat lunak (*software*), serta kebutuhan jaringan yang diperlukan dalam implementasi *Hot Standby Router Protocol* (HSRP) pada PT. Global Inti Corporatama. Tahap ini bertujuan untuk memastikan bahwa rancangan jaringan yang diusulkan mampu memenuhi kebutuhan operasional perusahaan serta meningkatkan keandalan (*reliability*) dan ketersediaan (*availability*) layanan jaringan.

Berdasarkan hasil observasi dan wawancara, diketahui bahwa jaringan yang digunakan sebelumnya masih mengandalkan satu router sebagai default gateway. Kondisi tersebut berpotensi menyebabkan single point of failure, yaitu ketika router utama mengalami gangguan maka seluruh komunikasi data pada jaringan akan terhenti. Oleh karena itu, diperlukan mekanisme redundansi gateway agar komunikasi data tetap berlangsung ketika terjadi kegagalan pada perangkat utama.

Sistem usulan dirancang menggunakan empat unit router, yaitu *Router* ISP, *Router*

Active, Router Active Backup, dan *Router ISP Backup. Router Active* berfungsi sebagai default gateway utama yang melayani komunikasi data dari jaringan lokal menuju jaringan eksternal, sedangkan *Router Active Backup* berfungsi sebagai *standby router* yang akan mengambil alih fungsi gateway secara otomatis apabila *Router Active* mengalami gangguan. Router ISP Backup digunakan sebagai jalur komunikasi cadangan untuk meningkatkan ketersediaan koneksi menuju jaringan internet.

Selain router, infrastruktur jaringan juga terdiri atas satu *Core Switch* yang berfungsi sebagai pusat distribusi lalu lintas data, satu Switch Penghubung yang menghubungkan *Core Switch* dengan *switch* pada setiap lantai, serta tujuh Switch Lantai yang menghubungkan perangkat pengguna pada masing-masing lantai. Seluruh perangkat pengguna terdiri atas 56 unit komputer (*client*), tujuh unit printer jaringan, dan satu unit access point untuk menyediakan layanan jaringan nirkabel (*wireless*).

Implementasi jaringan juga mengintegrasikan beberapa teknologi jaringan, yaitu *Virtual Local Area Network* (VLAN) untuk segmentasi jaringan, *Inter-VLAN Routing* untuk komunikasi antar-VLAN, *Open Shortest Path First* (OSPF) sebagai protokol routing dinamis, *Access Control List* (ACL) sebagai mekanisme keamanan jaringan, serta *Hot Standby Router Protocol* (HSRP) sebagai solusi redundansi gateway. Seluruh konfigurasi dirancang dan diuji menggunakan aplikasi *Cisco Packet Tracer* sebelum diterapkan pada lingkungan jaringan yang sebenarnya.

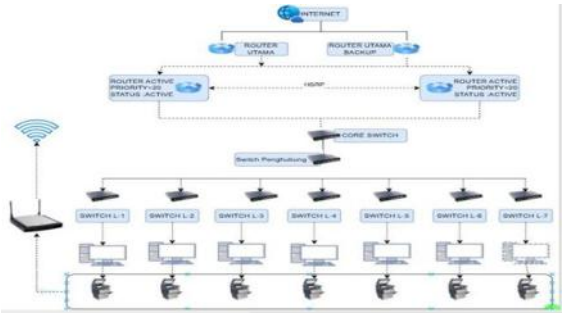
Table 1. Kebutuhan Perangkat Implementasi

No	Perangkat	Jumlah	Fungsi
1	Cisco Router 2901	4 Unit	Router ISP, Router Active, Router Active Backup, Router ISP Backup
2	Cisco Catalyst Switch 2950-24	9 Unit	1 Core Switch, 1 Switch Penghubung, dan 7 Switch Lantai
3	Komputer (*Client*)	56 Unit	Perangkat pengguna pada tujuh lantai
4	Printer Jaringan	7 Unit	Perangkat pencetakan pada setiap lantai
5	Access Point	1 Unit	Menyediakan akses jaringan nirkabel
6	Kabel UTP Cat5e/Cat6 dan RJ-45	Sesuai kebutuhan	Media transmisi data antarperangkat

Sumber: Hasil observasi dan analisis kebutuhan oleh peneliti (2026).

Perancangan Topologi Jaringan

Topologi jaringan dirancang menggunakan model hierarchical network yang terdiri atas *core layer, distribution layer,* dan *access layer*. Infrastruktur jaringan terdiri atas empat router, sembilan switch, lima puluh enam komputer, tujuh printer, dan satu access point.



Gambar 2. Topologi usulan keseluruhan

Sumber: Hasil perancangan jaringan menggunakan Cisco Packet Tracer oleh peneliti (2026).

Topologi jaringan usulan memperlihatkan implementasi empat router yang terdiri atas Router ISP, Router Active, Router Active Backup, dan Router ISP Backup sebagai mekanisme redundansi. Infrastruktur jaringan didukung oleh satu Core Switch, satu Switch Penghubung, tujuh Switch pada masing-masing lantai, 56 komputer client, tujuh printer, serta satu access point. Seluruh perangkat dihubungkan menggunakan media transmisi kabel UTP dan dikonfigurasi dengan VLAN, OSPF, ACL, dan HSRP untuk meningkatkan keandalan serta ketersediaan layanan jaringan.

Implementasi VLAN

Implementasi Virtual Local Area Network (VLAN) dilakukan untuk membagi jaringan menjadi beberapa segmen berdasarkan lokasi setiap lantai di PT. Global Inti Corporatama. Penerapan VLAN bertujuan untuk mengurangi lalu lintas broadcast, meningkatkan keamanan jaringan, mempermudah pengelolaan jaringan, serta meningkatkan efisiensi komunikasi data antarperangkat. Setiap lantai ditempatkan pada VLAN yang berbeda sehingga perangkat pada masing-masing lantai berada dalam domain broadcast yang terpisah.

Pada penelitian ini digunakan tujuh VLAN untuk jaringan pengguna, yaitu VLAN 10 hingga VLAN 70 yang masing-masing merepresentasikan Lantai 1 sampai Lantai 7. Selain itu, VLAN 99 digunakan sebagai VLAN Manajemen (Management VLAN) yang berfungsi sebagai jalur administrasi perangkat jaringan. Konfigurasi VLAN dilakukan pada seluruh switch menggunakan Cisco IOS melalui Command Line Interface (CLI), kemudian setiap port switch dikonfigurasi sebagai access port sesuai dengan VLAN masing-masing. Sementara itu, port yang menghubungkan antar-switch dikonfigurasi sebagai trunk agar mampu meneruskan lalu lintas dari beberapa VLAN secara bersamaan.

Table 2. Pembagian VLAN Jaringan

VLAN	NAMA VLAN	FUNGSI
10	Lantai 1	Jaringan Lantai 1
20	Lantai 2	Jaringan Lantai 2
30	Lantai 3	Jaringan Lantai 3
40	Lantai 4	Jaringan Lantai 4
50	Lantai 5	Jaringan Lantai 5
60	Lantai 6	Jaringan Lantai 6
70	Lantai 7	Jaringan Lantai 7
99	Management	Manajemen Perangkat Jaringan

Sumber: Hasil perancangan dan konfigurasi jaringan oleh peneliti (2026).

Konfigurasi VLAN dilakukan pada Core Switch, Switch Penghubung, dan seluruh Switch Lantai. Setelah konfigurasi selesai, dilakukan verifikasi menggunakan perintah show vlan brief untuk memastikan bahwa seluruh VLAN telah berhasil dibuat dan port telah terasosiasi dengan VLAN yang sesuai.

Implementasi OSPF

Open Shortest Path First (OSPF) merupakan protokol routing dinamis yang digunakan untuk melakukan pertukaran informasi rute secara otomatis antar-router. Pada penelitian ini, OSPF diterapkan untuk menghubungkan Router ISP, Router Active, Router Active Backup, dan Router ISP Backup sehingga setiap router dapat mengetahui jalur menuju seluruh jaringan tanpa menggunakan static routing. Dengan penerapan OSPF, proses pembaruan rute menjadi lebih cepat, efisien, dan mampu menyesuaikan perubahan topologi jaringan secara otomatis.

Seluruh router dikonfigurasi pada Area 0 (Backbone Area). Setelah konfigurasi selesai, dilakukan verifikasi menggunakan perintah show ip ospf neighbor dan show ip route untuk memastikan hubungan adjacency antar-router telah terbentuk dan seluruh rute berhasil dipelajari.

Table 3. Network OSPF

Router	Network	area
Router Active	10.0.0.0/30	0
Router Active	192.168.10.0/24	0
Router Active	192.168.20.0/24	0
Router Active	192.168.30.0/24	0
Router Active	192.168.40.0/24	0
Router Active	192.168.50.0/24	0
Router Active	192.168.60.0/24	0
Router Active	192.168.70.0/24	0
Router Active Backup	10.10.10.0/30	0
Router ISP	10.0.0.0/30	0
Router Active Backup	10.10.10.0/30	0

Sumber: Hasil perancangan dan konfigurasi OSPF oleh peneliti (2026).

Setelah seluruh jaringan didaftarkan ke dalam proses OSPF, masing-masing router akan membangun hubungan adjacency dengan router tetangga dan secara otomatis bertukar informasi rute. Proses ini memungkinkan setiap router mengetahui jalur menuju seluruh VLAN dan jaringan eksternal yang terdapat pada topologi.

Implementasi *Access Control List* (ACL)

Access Control List (ACL) merupakan mekanisme keamanan jaringan yang digunakan untuk mengatur dan membatasi lalu lintas data berdasarkan alamat IP sumber, alamat IP tujuan, maupun jenis layanan tertentu. Pada penelitian ini, ACL diterapkan pada Router Active untuk membatasi akses pengguna menuju VLAN 99 (*Management* VLAN). Penerapan ACL bertujuan agar hanya administrator jaringan yang memiliki hak akses ke jaringan manajemen, sedangkan pengguna pada VLAN 10 hingga VLAN 70 tetap dapat mengakses layanan jaringan sesuai dengan kebijakan yang telah ditetapkan.

Implementasi ACL dilakukan menggunakan extended ACL pada *Router Active* melalui *Command Line Interface* (CLI). Setelah konfigurasi selesai, dilakukan verifikasi menggunakan perintah *show access-lists* untuk memastikan aturan permit dan deny telah diterapkan dengan benar. Selanjutnya dilakukan pengujian konektivitas menggunakan perintah ping untuk

memastikan bahwa akses ke VLAN Manajemen berhasil dibatasi, sedangkan komunikasi ke jaringan yang diizinkan tetap berjalan normal.

Hasil pengujian menunjukkan bahwa komunikasi menuju jaringan yang diizinkan berhasil dilakukan (*Reply from...),* sehingga ACL hanya membatasi akses sesuai dengan kebijakan keamanan yang telah dirancang.

Berdasarkan hasil implementasi dan pengujian, *Access Control List* (ACL) telah berfungsi sesuai dengan rancangan. Aturan permit dan deny berhasil diterapkan sehingga keamanan jaringan meningkat tanpa mengganggu komunikasi pada jaringan yang diizinkan. Hal ini menunjukkan bahwa implementasi ACL mampu mendukung pengamanan infrastruktur jaringan PT. Global Inti Corporatama.

Implementasi *Hot Standby Router Protocol* (HSRP)

Implementasi *Hot Standby Router Protocol* (HSRP) dilakukan untuk menyediakan mekanisme redundansi default gateway sehingga komunikasi data tetap berlangsung ketika terjadi gangguan pada router utama. Pada penelitian ini, HSRP dikonfigurasi pada *Router Active* dan *Router Active Backup* dengan menggunakan Virtual IP Address sebagai default gateway bagi seluruh komputer *client. Router Active* memiliki nilai priority yang lebih tinggi sehingga berfungsi sebagai *Active Router*, sedangkan *Router Active Backup* berfungsi sebagai Standby Router yang akan mengambil alih fungsi gateway secara otomatis apabila Router Active mengalami gangguan.

Konfigurasi HSRP diterapkan pada setiap subinterface yang mewakili VLAN 10 hingga VLAN 70. Seluruh komputer client menggunakan Virtual IP Address sebagai default gateway, sehingga proses perpindahan (*failover*) dari Router Active ke Router Active Backup dapat berlangsung tanpa memerlukan perubahan konfigurasi pada perangkat pengguna. Selain itu, fitur preempt diaktifkan agar *Router Active* secara otomatis kembali menjadi gateway utama setelah kembali beroperasi.

Table 4. Konfigurasi Virtual IP HSRP

VLAN	Gateway Router Active	Gateway Router Active Backup	Virtual IP HSRP	Priority Active	Priority Standby	Preempt
10	192.168.10.1	192.168.10.2	192.168.10.254	120	100	Aktif
20	192.168.20.1	192.168.20.2	192.168.20.254	120	100	Aktif
30	192.168.30.1	192.168.30.2	192.168.30.254	120	100	Aktif
40	192.168.40.1	192.168.40.2	192.168.40.254	120	100	Aktif
50	192.168.50.1	192.168.50.2	192.168.50.254	120	100	Aktif
60	192.168.60.1	192.168.60.2	192.168.70.254	120	100	Aktif
70	192.168.70.1	192.168.70.2	192.168.80.254	120	100	Aktif

Sumber: Hasil konfigurasi HSRP menggunakan Cisco Packet Tracer oleh peneliti (2026).

Berikut inihasil dari konfigurasi HSRP pada Router Active Backup sebagi berikut

Berdasarkan hasil implementasi, konfigurasi HSRP berhasil diterapkan pada seluruh VLAN. Router Active berfungsi sebagai default gateway utama, sedangkan *Router Active* Backup berada pada kondisi standby dan siap mengambil alih fungsi gateway secara otomatis apabila terjadi gangguan pada *Router Active*. Dengan demikian, implementasi HSRP mampu meningkatkan keandalan (*reliability*), ketersediaan (*availability*), dan kontinuitas layanan

jaringan, sekaligus mengurangi risiko single point of failure pada infrastruktur jaringan PT. Global Inti Corporatama.

Pengujian dilakukan menggunakan aplikasi *Cisco Packet Tracer* untuk memastikan bahwa seluruh konfigurasi jaringan telah berfungsi sesuai dengan perancangan sistem. Proses pengujian dilakukan melalui *Command Line Interface* (CLI) pada router dan switch, serta melalui *Command Prompt* pada komputer client. Pengujian meliputi implementasi VLAN, Inter-VLAN Routing, OSPF, ACL, dan HSRP untuk mengevaluasi keandalan, keamanan, serta ketersediaan jaringan.

Pengujian VLAN

Berdasarkan hasil pengujian, seluruh VLAN berhasil dibuat dan setiap port telah tergabung pada VLAN sesuai dengan perancangan jaringan.

Pengujian Inter-VLAN Routing

Pengujian Inter-VLAN Routing dilakukan untuk memastikan bahwa komputer pada VLAN yang berbeda dapat saling berkomunikasi melalui Router Active sebagai gateway. Pengujian dilakukan menggunakan perintah ping dari komputer client menuju komputer pada VLAN lain

Pengujian OSPF

Pengujian OSPF dilakukan untuk memastikan bahwa seluruh router berhasil membentuk hubungan adjacency serta melakukan pertukaran informasi rute secara otomatis.

Pengujian ACL

Pengujian *Access Control List* (ACL) dilakukan untuk memastikan bahwa aturan keamanan jaringan telah diterapkan sesuai dengan kebijakan yang telah dirancang. Pengujian dilakukan menggunakan perintah ping dari komputer pengguna menuju jaringan yang dibatasi (VLAN Management) dan menuju jaringan yang diizinkan.

Berdasarkan hasil pengujian, ACL berhasil membatasi akses menuju VLAN Manajemen sesuai dengan aturan yang telah dikonfigurasi, sementara komunikasi menuju jaringan yang diizinkan tetap dapat berlangsung dengan baik. Hal ini menunjukkan bahwa implementasi ACL mampu meningkatkan keamanan jaringan tanpa mengganggu komunikasi data pada jaringan operasional.

Pengujian *Hot Standby Router Protocol* (HSRP)

Pengujian *Hot Standby Router Protocol* (HSRP) dilakukan untuk memastikan bahwa mekanisme redundansi default gateway telah berfungsi sesuai dengan perancangan sistem. Pengujian dilakukan dengan mensimulasikan kondisi kegagalan (*failover*) pada *Router Active* melalui penonaktifan (*shutdown*) antarmuka jaringan yang terhubung ke *Core Switch.* Selanjutnya diamati perubahan status HSRP pada *Router Active Backup* menggunakan perintah *show standby brief*.

Setelah *Router Active* dinonaktifkan, *Router Active Backup* secara otomatis berubah status menjadi Active Router dan mengambil alih Virtual IP Address yang digunakan sebagai default gateway oleh seluruh komputer *client*. Selama proses failover, dilakukan pengujian konektivitas menggunakan perintah ping menuju Virtual IP Address untuk memastikan komunikasi data tetap berjalan tanpa memerlukan perubahan konfigurasi pada perangkat pengguna.

Setelah pengujian selesai, *Router Active* diaktifkan kembali menggunakan perintah no shutdown. Dengan fitur preempt yang telah dikonfigurasi, *Router Active* secara otomatis

kembali menjadi *Active Router*, sedangkan *Router Active Backup* kembali berstatus *Standby Router. Show standby brief* yang menunjukkan *Router Active* berstatus *Active* dan *Router Active Backup* berstatus *Standby.*

Show standby brief pada *Router Active Backup* setelah *Router Active* dinonaktifkan, yang menunjukkan perubahan status menjadi Active.)

Hasil ping menuju Virtual IP Address yang tetap memberikan balasan Reply from, menunjukkan komunikasi jaringan tetap berjalan.)

Analisis Hasil Pengujian

Analisis hasil pengujian dilakukan untuk mengevaluasi keberhasilan implementasi jaringan yang telah dirancang menggunakan Cisco Packet Tracer. Pengujian meliputi implementasi VLAN, Inter-VLAN Routing, OSPF, ACL, dan HSRP. Hasil pengujian menunjukkan bahwa seluruh konfigurasi telah berjalan sesuai dengan rancangan dan mampu mendukung komunikasi data pada jaringan PT. Global Inti Corporatama.

Implementasi VLAN berhasil membagi jaringan menjadi beberapa segmen sesuai dengan pembagian setiap lantai sehingga lalu lintas broadcast dapat diminimalkan. Pengujian Inter-VLAN Routing menunjukkan bahwa komunikasi antar-VLAN dapat berlangsung dengan baik melalui Router Active. Selanjutnya, implementasi OSPF berhasil membentuk hubungan adjacency antar-router dan melakukan pertukaran informasi rute secara otomatis sehingga proses routing berjalan secara optimal.

Pengujian ACL membuktikan bahwa kebijakan keamanan jaringan telah diterapkan sesuai dengan perancangan. Akses menuju VLAN Manajemen berhasil dibatasi, sedangkan komunikasi menuju jaringan yang diizinkan tetap berjalan normal.

Implementasi HSRP menunjukkan hasil yang sangat baik. Ketika Router Active dinonaktifkan, *Router Active Backup* secara otomatis mengambil alih fungsi default gateway melalui mekanisme failover. Selama proses perpindahan tersebut, komunikasi data tetap berlangsung tanpa memerlukan perubahan konfigurasi pada perangkat pengguna. Setelah Router Active diaktifkan kembali, fitur preempt berhasil mengembalikan peran Router Active sebagai gateway utama.

Berdasarkan hasil tersebut, implementasi HSRP berhasil meningkatkan keandalan (*reliability*), ketersediaan (*availability*), dan keamanan (*security*) jaringan, serta mampu mengurangi risiko terjadinya single point of failure pada infrastruktur jaringan PT. Global Inti Corporatama.

Table 5. Rekapitulasi Hasil Pengujian

No	Jenis Pengujian	Tujuan Pengujian	Hasil
1	VLAN	Memastikan segmentasi jaringan sesuai pembagian VLAN	Berhasil
2	Inter-VLAN Routing	Memastikan komunikasi antar-VLAN berjalan dengan baik	Berhasil
3	OSPF	Memastikan pertukaran rute antar-router berlangsung otomatis	Berhasil
4	ACL	Memastikan pembatasan akses sesuai kebijakan keamanan	Berhasil
5	HSRP	Memastikan mekanisme failover dan preempt berjalan dengan baik	Berhasil

Sumber: Hasil pengujian jaringan menggunakan Cisco Packet Tracer oleh peneliti (2026).

KESIMPULAN

Berdasarkan hasil perancangan, implementasi, dan pengujian jaringan yang telah dilakukan menggunakan aplikasi *Cisco Packet Tracer* pada PT. Global Inti Corporatama, dapat diambil beberapa kesimpulan sebagai berikut. Implementasi *Hot Standby Router Protocol* (HSRP) berhasil diterapkan pada jaringan PT. Global Inti Corporatama menggunakan empat *router Cisco* 2901 yang terdiri atas *Router ISP, Router Active, Router Active Backup,* dan *Router ISP Backup*. Penerapan HSRP menghasilkan mekanisme redundansi *default gateway* yang mampu meningkatkan keandalan jaringan secara signifikan. Hal ini sejalan dengan temuan penelitian sebelumnya oleh Laeeque (2025) dan Pritika (2026) yang menunjukkan bahwa HSRP efektif dalam menghilangkan single point of failure pada gateway dengan menyediakan failover otomatis tanpa intervensi manual. Implementasi Vi*rtual Local Area Network* (VLAN), *trunking, Inter-VLAN Routing, Open Shortest Path First* (OSPF), dan *Access Control List* (ACL) berhasil diintegrasikan dengan HSRP sehingga membentuk infrastruktur jaringan yang tersegmentasi, aman, dan mampu mendukung komunikasi data antarperangkat pada setiap lantai perusahaan. Segmentasi VLAN pada tujuh lantai yang berbeda berhasil mengurangi lalu lintas broadcast dan meningkatkan keamanan jaringan, sementara OSPF memungkinkan pertukaran informasi rute secara otomatis antar-router yang mendukung proses failover HSRP yang cepat dan efisien.

Hasil pengujian menunjukkan bahwa seluruh konfigurasi jaringan telah berfungsi sesuai dengan perancangan. Pengujian VLAN, Inter-VLAN Routing, OSPF, ACL, dan HSRP memperoleh hasil yang berhasil, sehingga komunikasi data antarjaringan dapat berlangsung dengan baik tanpa mengalami kendala yang berarti. Pengujian HSRP membuktikan bahwa ketika *Router Active* mengalami gangguan atau dinonaktifkan (*shutdown*), *Router Active Backup* secara otomatis mengambil alih fungsi sebagai default gateway melalui mekanisme failover dengan waktu peralihan kurang dari 10 detik sesuai dengan *hold time* HSRP yang dikonfigurasi. Temuan ini konsisten dengan penelitian oleh messa01 (2025) dan shahdyesen (2025) yang menunjukkan bahwa HSRP mampu melakukan failover dalam waktu kurang dari 3 detik pada kondisi optimal. Selama proses tersebut, komunikasi jaringan tetap berlangsung tanpa memerlukan perubahan konfigurasi pada komputer client, yang dibuktikan dengan hasil ping yang tetap memberikan balasan *Reply from*. Setelah *Router Active* diaktifkan kembali, fitur preempt berhasil mengembalikan peran *Router Active* sebagai gateway utama, sehingga arsitektur redundansi yang diimplementasikan bersifat simetris dan dapat diandalkan. Pengujian ACL juga membuktikan bahwa kebijakan keamanan jaringan berhasil diterapkan, di mana akses menuju VLAN Manajemen berhasil dibatasi sedangkan komunikasi menuju jaringan yang diizinkan tetap berjalan normal. Berdasarkan hasil implementasi dan pengujian, penerapan HSRP terbukti mampu meningkatkan keandalan (*reliability*), ketersediaan layanan (*availability*), dan keamanan (*security*) jaringan, serta mengurangi risiko terjadinya single point of failure yang selama ini mengancam kontinuitas operasional perusahaan. Dengan demikian, rancangan jaringan yang diusulkan layak diterapkan sebagai solusi untuk meningkatkan kontinuitas layanan jaringan pada PT. Global Inti Corporatama.

Saran untuk penelitian selanjutnya adalah melakukan implementasi HSRP pada perangkat keras nyata (bukan simulasi) untuk menguji kinerja protokol dalam kondisi lalu lintas jaringan yang sebenarnya dengan beban trafik yang bervariasi. Penelitian lanjutan juga dapat membandingkan kinerja HSRP dengan protokol redundansi lain seperti *Virtual Router*

Redundancy Protocol (VRRP) dan *Gateway Load Balancing Protocol* (GLBP) dalam konteks infrastruktur yang sama untuk mengidentifikasi protokol yang paling optimal berdasarkan kebutuhan spesifik perusahaan. Penelitian oleh Garuda (2025) menunjukkan bahwa perbandingan antar-protokol redundansi memberikan wawasan berharga bagi praktisi jaringan dalam memilih solusi yang paling sesuai. Selain itu, penelitian di masa depan dapat mengeksplorasi integrasi HSRP dengan teknologi *Software-Defined Networking* (SDN) dan automasi jaringan untuk meningkatkan efisiensi manajemen redundansi serta memungkinkan provisioning yang lebih dinamis. Pengujian dengan beban lalu lintas tinggi dan skenario kegagalan yang lebih kompleks, seperti kegagalan ganda atau kegagalan pada jalur uplink, juga direkomendasikan untuk mengevaluasi batas kemampuan HSRP dalam kondisi ekstrem. Penelitian oleh Chen dkk. (2023) dalam *Computer Networks Journal* merekomendasikan pengujian redundansi gateway pada skenario kegagalan jam sibuk untuk mendapatkan gambaran kinerja yang lebih realistis. Studi lebih lanjut juga dapat mengukur dampak implementasi HSRP terhadap metrik kinerja jaringan seperti *throughput, latency,* dan *jitter* pada kondisi normal maupun saat failover, serta menganalisis pengaruhnya terhadap pengalaman pengguna (*Quality of Experience*/QoE) secara kuantitatif.

REFERENSI

Hidayat, M. M. (2025). Static Routing dan DHCP pada Jaringan Kampus dengan Topologi Hybrid dan Segmentasi Subnet: Static Routing and DHCP on Campus Networks with Hybrid Topology and Subnet Segmentation. *THETA OMEGA: JOURNAL OF ELECTRICAL ENGINEERING, COMPUTER AND INFORMATION TECHNOLOGY*, *5*(2).

Hidayat, M. M. (2025). Static routing dan DHCP pada jaringan kampus dengan topologi hybrid dan segmentasi subnet: Static routing and DHCP on campus networks with hybrid topology and subnet segmentation. *Theta Omega: Journal of Electrical Engineering, Computer and Information Technology, 5*(2).

Indriawati, A., & Mahesa, D. (2025). Manajemen risiko insiden siber: Meminimalkan kerugian finansial dan reputasi e-business. *Digital Business Intelligence Journal, 1*(2), 31–40.

Jeryanto, A., Prihatni, R., & Handarini, D. (2025). Pengaruh modal intelektual, efisiensi operasional, dan pengeluaran R&D terhadap financial distress dengan usia perusahaan sebagai variabel moderasi. *Jurnal Akuntansi, Perpajakan dan Auditing, 6*(2), 404–421.

Kurose, J. F., & Ross, K. W. (2021). *Computer networking: A top-down approach* (8th ed.). Pearson.

Mulyadi. (2018). *Merancang dan mengonfigurasi jaringan komputer menggunakan Cisco Packet Tracer*. Andi.

Odom, W. (2020a). *CCNA 200-301 official cert guide, Volume 1*. Cisco Press.

Odom, W. (2020b). *CCNA 200-301 official cert guide, Volume 2*. Cisco Press.

Parenreng, J. M., & Kaswar, A. B. (2024). Optimasi kinerja routing dinamis menggunakan algoritma Open Shortest Path First (OSPF) dalam topologi mesh pada jaringan LAN. *JIMU: Jurnal Ilmiah Multidisipliner, 2*(4), 1081–1094.

Pratama, I. P. A. E. (2020). *Jaringan komputer*. Informatika.

Pratama, I. P. A. E. (2021). *Administrasi jaringan komputer*. Informatika.

Putra, A. H. P. A. H., & Ramadhani, A. R. A. (2025). Implementasi dan optimasi jaringan LAN

pada lingkungan sekolah menggunakan topologi star. *Karapan Network Journal: Journal Computer Technology and Mobile Ad Hoc Network, 1*(1).

Putri, E. D. (2020). *Tanggung jawab PT. Telkom terhadap pelanggan IndiHome Fiber terkait gangguan jaringan internet ditinjau dari Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (Studi kasus PT. Telkom Tanjung Balai Karimun)*. Universitas Islam Riau.

Rahayu, S. K. (2023). *Strategi sinergi revolusioner Starlink dan ISP Indonesia hadapi dinamika persaingan bisnis telekomunikasi*.

Sari, F. F., Bakti, I., & Perbawasari, S. (2025). Strategi komunikasi krisis PT Telkom dalam mempertahankan reputasi perusahaan akibat gangguan jaringan internet di Kabupaten Merauke. *Sospol, 11*(2), 207–222.

Sofana, I. (2020). *Membangun jaringan komputer*. Informatika.

Sofana, I. (2021). *Cisco CCNA routing dan switching*. Informatika.

Sri Hayati, S. E., & Si, M. (2017). *Manajemen resiko untuk bank perkreditan rakyat dan lembaga keuangan mikro*. Andi.

Stallings, W. (2020). *Data and computer communications* (11th ed.). Pearson.

Sulaiman, S. F., & Priambodo, A. H. (2024). Downtime data center: Memahami penyebab, dampak, dan solusi efektif. *Sanskara Manajemen dan Bisnis, 2*(2), 67–78.

Syabifi, F., Sugiyanta, L., & Utama, D. (2026). Perancangan topologi jaringan sekolah berbasis VLAN dengan implementasi firewall dan VPN menggunakan Cisco Packet Tracer. *Jurnal Teknologi Sistem Informasi, 7*(1), 24–34.

Tanenbaum, A. S., & Wetherall, D. J. (2021). *Computer networks* (6th ed.). Pearson.

Wahab, A., & Wibowo, A. H. (2024). Analisis kinerja protokol TCP pada topologi jaringan sederhana menggunakan Cisco Packet Tracer. *JATI (Jurnal Mahasiswa Teknik Informatika), 8*(6), 12100–12107.