**TeknoIS: Jurnal Ilmiah Teknologi Informasi dan Sains**
Volume 16 Number 2, July 2026 Page. 215-223
Journal Homepage: https://teknois.unbin.ac.id/index.php/JBS/
Received: April 2026; Accepted: July 2026; Published: July 2026

# Evaluasi Infrastruktur Jaringan Komputer Menggunakan PPDIOO pada Badan Pendapatan Daerah Kabupaten Majalengka

**Fauzan Ahmad Arhaburrizqi[1*], Fahmi Adib Nabhan[2], Helmy Dzulfikar[3]**
[1,2,3] Sistem Informasi/Fakultas Teknik/Universitas Siliwangi
[1]Email: fauzanahmad0520@gmail.com
[2]Email: fahmicms16@gmail.com
[3]Email: helmydz@unsil.ac.id

*) *Corresponding Author*

***ABSTRACT***

*This study aims to evaluate the computer network infrastructure and formulate a redesign at the Regional Revenue Agency of Majalengka Regency to mitigate system failure risks due to reliance on a single internet service provider. The novelty of this research lies in the execution of the complete network development lifecycle, encompassing the preparation, planning, design, implementation, operation, and optimization phases. Given the critical nature of government agency operations requiring zero downtime, the implementation, operation, and optimization phases were fully realized within a virtual simulation environment using Cisco Packet Tracer software. Evaluation results indicate that although the existing infrastructure has adequate logical network segmentation and automated addressing, the absence of a backup connection line remains a primary vulnerability. As a solution, this study produces an architectural recommendation that integrates a secondary internet service provider with an automated connection switching configuration. Simulation results prove that the proposed design successfully maintains smooth data traffic during disruptions, thereby ensuring the continuous availability of digital tax services.*

***Keywords***: *automated connection switching; cisco packet tracer; infrastructure evaluation; network design; tax services*

**ABSTRAK**

Penelitian ini bertujuan untuk mengevaluasi infrastruktur jaringan komputer dan merumuskan desain perbaikan pada Badan Pendapatan Daerah Kabupaten Majalengka guna memitigasi risiko kegagalan sistem akibat ketergantungan pada satu penyedia layanan internet. Kebaruan penelitian ini terletak pada eksekusi siklus hidup pengembangan jaringan secara utuh yang mencakup tahapan persiapan, perencanaan, perancangan, implementasi, operasional, hingga optimasi. Mengingat krusialnya operasional instansi pemerintah yang menuntut kondisi nihil waktu henti, fase implementasi, operasional, dan optimasi direalisasikan sepenuhnya di dalam lingkungan simulasi virtual menggunakan perangkat lunak Cisco Packet Tracer. Hasil evaluasi menunjukkan bahwa meski infrastruktur eksisting telah memiliki segmentasi jaringan logis dan pengalamatan otomatis yang memadai, ketiadaan jalur koneksi cadangan menjadi titik rentan utama. Sebagai solusi, penelitian ini menghasilkan rekomendasi arsitektur yang mengintegrasikan penyedia layanan internet sekunder dengan konfigurasi mekanisme peralihan koneksi otomatis. Hasil simulasi membuktikan bahwa desain usulan berhasil menjaga kelancaran lalu lintas data saat terjadi gangguan, sehingga ketersediaan akses untuk layanan perpajakan digital tetap terjamin.

***Keywords***: *cisco packet tracer; desain jaringan; evaluasi infrastruktur; layanan perpajakan; peralihan koneksi otomatis*

**TeknoIS: Jurnal Ilmiah Teknologi Informasi dan Sains**
Volume 16 Number 2, July 2026 Page. 215-223
Journal Homepage: https://teknois.unbin.ac.id/index.php/JBS/
Received: April 2026; Accepted: July 2026; Published: July 2026

## A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi mendorong transformasi digital secara masif di sektor pemerintahan. Infrastruktur jaringan komputer menjadi tulang punggung operasional yang menunjang layanan publik secara cepat, transparan, dan akuntabel. Badan Pendapatan Daerah (Bapenda) memikul tanggung jawab strategis dalam mengelola Pendapatan Asli Daerah (PAD), termasuk Pajak Bumi dan Bangunan (PBB) serta Bea Perolehan Hak atas Tanah dan Bangunan (BPHTB). Bapenda Kabupaten Majalengka telah mengimplementasikan bermacam inovasi digital, seperti sistem SIMPEL PBB (Sistem Pelayanan PBB *Online*) dan integrasi pembayaran menggunakan *Quick Response Code Indonesian Standard* (QRIS). Sebagai mesin penggerak program Percepatan dan Perluasan Digitalisasi Daerah (P2DD), operasional instansi ini sangat bergantung pada stabilitas infrastruktur jaringan. Urgensi dan rasionalisasi dari kegiatan ini didasari oleh fakta bahwa operasional jaringan Bapenda sempat mengalami kendala teknis berupa *downtime*. Performa jaringan eksisting yang tidak optimal, seperti tingginya latensi atau ketidakstabilan koneksi *provider*, berpotensi menghambat efisiensi operasional sistem yang kini seluruhnya berbasis online, menurunkan kredibilitas layanan, dan memicu kerentanan terhadap keamanan data perpajakan yang bersifat sensitif. Oleh karena itu, evaluasi terstruktur menjadi keharusan untuk memastikan tidak adanya hambatan dalam pelayanan publik.

Upaya optimalisasi infrastruktur jaringan melalui metodologi terstruktur telah banyak dikaji secara ilmiah, khususnya dalam mengatasi masalah stabilitas koneksi dan keamanan arus data. Dari aspek stabilitas layanan, implementasi kerangka kerja PPDIOO terbukti efektif dalam meminimalkan downtime pertukaran data terpusat dan meningkatkan parameter *Quality of Service* (QoS) pada jaringan intra-pemerintah secara signifikan [1], [2]. Evaluasi terhadap topologi di tahap awal perencanaan PPDIOO juga menjadi langkah pencegahan yang krusial agar tidak terjadi *bottleneck* atau kemacetan lalu lintas data yang kerap mengganggu produktivitas layanan operasional [3].

Selain memastikan kelancaran koneksi, penanganan data berskala institusi yang sensitif menuntut rancangan infrastruktur yang aman. Kajian terdahulu menegaskan bahwa pemisahan hak akses dan efisiensi pengalamatan IP melalui segmentasi jaringan (Variable Length Subnet Masking) sangat ideal dimodelkan menggunakan pendekatan PPDIOO [4], [5]. Lebih jauh lagi, mitigasi keamanan di level router gateway melalui penerapan *firewall rules* terbukti sangat esensial untuk mencegah serangan jaringan seperti DOS (*Denial of Service*) yang berpotensi melumpuhkan sistem *e-government* [6].

Berdasarkan tinjauan terhadap penelitian terdahulu tersebut, dapat ditarik benang merah bahwa metodologi PPDIOO sangat relevan untuk membedah masalah di Bapenda Majalengka. Sebagai penegasan kebaruan (*novelty*), evaluasi ini mengeksekusi siklus hidup PPDIOO secara utuh. Guna meminimalisasi risiko gangguan operasional pada jaringan fisik eksisting yang menuntut kondisi *zero downtime*, tahapan validasi akhir yang mencakup fase *Implement, Operate*, dan *Optimize* (IOO) diisolasi dan dieksekusi sepenuhnya di dalam lingkungan simulasi *Cisco Packet Tracer*. Penerapan metodologi terstruktur ini memberikan panduan dalam mengelola infrastruktur teknologi secara efisien, serta memastikan bahwa desain yang dihasilkan memenuhi kriteria keamanan dan ketersediaan sumber daya jaringan yang handal [7]. Penelitian ini secara spesifik bertujuan untuk mengidentifikasi dan mendokumentasikan kondisi parameter topologi jaringan, skema pengalamatan *Internet Protocol* (IP), kapabilitas konektivitas, serta keamanan dasar (*firewall rules*). Melalui simulasi PPDIOO yang komprehensif, evaluasi ini diharapkan mampu mengisolasi titik penyumbatan (*bottleneck*) dan celah keamanan secara akurat, sehingga menghasilkan rekomendasi arsitektur jaringan usulan yang teruji kestabilannya untuk menopang beban ekosistem *e-government*.

**TeknoIS: Jurnal Ilmiah Teknologi Informasi dan Sains**
Volume 16 Number 2, July 2026 Page. 215-223
Journal Homepage: https://teknois.unbin.ac.id/index.php/JBS/
Received: April 2026; Accepted: July 2026; Published: July 2026

## B. METODE

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan strategi studi kasus. Menurut Sugiyono [8], metode penelitian kualitatif digunakan untuk meneliti kondisi objek yang alamiah, di mana peneliti berperan sebagai instrumen kunci dan hasil kajian lebih ditekankan pada makna faktual. Seluruh proses pengumpulan data lapangan, perancangan, hingga validasi diintegrasikan ke dalam metodologi kerangka kerja PPDIOO (*Prepare, Plan, Design, Implement, Operate, Optimize*) berskala hibrida. Pendekatan ini memadukan evaluasi fisik di lapangan dengan validasi eksekusi akhir di dalam lingkungan simulasi virtual.

### 1. OBJEK, INSTRUMEN, DAN LINGKUNGAN SIMULASI

Penelitian ini dilaksanakan di lingkungan kantor Bapenda Kabupaten Majalengka (Jl. Raya Cigasong-Jatiwangi). Populasi dalam kajian ini mencakup keseluruhan ekosistem jaringan operasional instansi, dengan sampel ditentukan menggunakan teknik *purposive sampling*, di mana informan kuncinya adalah staf ahli *Information Technology* (IT) Bapenda. Fokus evaluasi dibatasi pada parameter teknis jaringan, tanpa mencakup evaluasi fungsionalitas sistem perangkat lunak (seperti SIMPEL PBB).

Instrumen pengumpulan data mencakup observasi dan wawancara mendalam. Bahan dan perangkat keras operasional yang menjadi sasaran evaluasi meliputi *router*, *switch*, *access point*, unit perlindungan *firewall*, serta infrastruktur penyimpanan terpusat *Network Attached Storage* (NAS) merek *Synology* berspesifikasi 4-bay dengan kapasitas 2 Terabita. Digunakan instrumen perangkat lunak Cisco Packet Tracer untuk menguji efikasi arsitektur usulan secara virtual.

### 2. TAHAPAN KERANGKA KERJA PPDIOO

Untuk menghindari risiko *downtime* pada operasional sistem *e-government* Bapenda yang sedang berjalan, siklus PPDIOO diaplikasikan secara penuh dengan fase implementasi hingga optimasi dilakukan murni secara virtual. Alur operasional dijabarkan sebagai berikut.

*Prepare* dilakukan untuk mengidentifikasi kendala struktural jaringan eksisting, riwayat downtime, dan kebutuhan lalu lintas data melalui wawancara dan observasi. Kemudian *planning* audit terhadap infrastruktur yang ada. Selanjutnya *design* rancangan topologi usulan yang mencakup segmentasi logis (*Virtual Local Area Network*/VLAN), serta mitigasi *firewall rules* untuk menjamin keamanan dasar jaringan. Lanjut *implement* dari desain tersebut di Cisco, yang mencakup tahapan penempatan perangkat jaringan virtual, penarikan media transmisi logis, dan input konfigurasi pengalamatan. Lalu *operate* di Cisco untuk memvalidasi konektivitas, menggunakan protokol diagnostik (seperti tes *Ping*) untuk memastikan kelancaran arus data. Terakhir *optimize* berdasarkan hasil uji operasi di simulator. Konfigurasi jaringan dikalibrasi ulang jika ditemukan *bottleneck* hingga mencapai parameter stabilitas dan keamanan maksimal sebelum direkomendasikan kepada pihak Bapenda.

### 3. TEKNIK ANALISIS DATA

Data lapangan dianalisis dengan prosedur kualitatif interaktif meliputi tiga tahapan. Pertama, reduksi data untuk menyaring dan menyederhanakan temuan mentah dari hasil wawancara terkait kendala teknis serta dokumentasi observasi fisik perangkat. Kedua, penyajian data dalam bentuk visualisasi topologi yang ada terstruktur. Ketiga, penarikan kesimpulan, di mana hasil analisis celah sistem ini secara sistematis diverifikasi dan dijadikan rumusan parameter wajib dalam menyusun rekomendasi arsitektur perbaikan jaringan pada fase *Design*.

## C. HASIL DAN PEMBAHASAN

### 1. HASIL

**KONDISI INFRASTRUKTUR JARINGAN EKSISTING**

**TeknoIS: Jurnal Ilmiah Teknologi Informasi dan Sains**
Volume 16 Number 2, July 2026 Page. 215-223
Journal Homepage: https://teknois.unbin.ac.id/index.php/JBS/
Received: April 2026; Accepted: July 2026; Published: July 2026

Berdasarkan hasil observasi dan wawancara dengan pengelola infrastruktur jaringan di Badan Pendapatan Daerah (Bapenda) Kabupaten Majalengka, instansi tersebut telah memanfaatkan berbagai perangkat keras jaringan guna mendukung operasional layanan digital perpajakan daerah, seperti SIMPEL PBB dan program P2DD. Rincian spesifikasi perangkat keras utama yang beroperasi saat ini disajikan pada Tabel 1.

Tabel 1. Spesifikasi Perangkat Jaringan Eksisting

| **Jenis Perangkat** | **Spesifikasi** | **Fungsi** |
|---|---|---|
| *Router* | Cisco 1941 | Menghubungkan jaringan internal ke ISP |
| *Firewall* | Cisco 5505 ASA | Melindungi jaringan dari ancaman eksternal |
| *Switch* | Cisco 3560 (*Core*) & 2960 (*Access*) | Distribusi koneksi ke perangkat klien |
| *Access Point* | *Access Point-PT-AC* | Menyediakan akses nirkabel untuk staf dan tamu |
| *Network Attached Storage* (NAS) | Synology (4 bay, 2 TB) | Penyimpanan file terpusat |
| *Internet Service Provider* (ISP) | Gisaka | Koneksi internet utama |

Secara teknis, jaringan di Bapenda Majalengka telah dikonfigurasi dengan menerapkan *Dynamic Host Configuration Protocol* (DHCP) untuk otomasi pengalamatan IP. Selain itu, telah dilakukan pemisahan hak akses antara staf, kepala badan, dan tamu (publik), serta pemanfaatan *Network Attached Storage* (NAS) merek Synology berkapasitas 2 TB sebagai pusat penyimpanan data.

## EVALUASI INFRASTRUKTUR

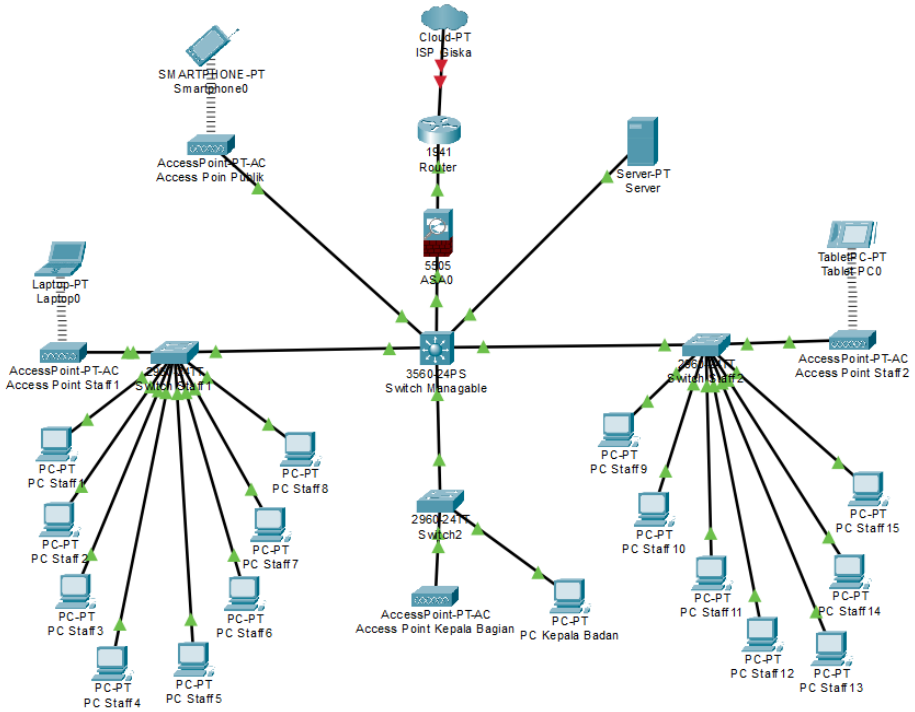
Melalui tahap *Prepare* dan *Plan* dalam metodologi PPDIOO, dilakukan identifikasi kebutuhan layanan dan audit terhadap infrastruktur yang berjalan. Layanan perpajakan daerah menuntut koneksi internet yang memiliki tingkat ketersediaan tinggi serta keamanan data yang ketat. Namun, hasil audit mengungkap beberapa permasalahan operasional, sebagaimana dirangkum pada Tabel 2.

Tabel 2. Hasil Audit Infrastruktur Eksisting

| **Aspek** | **Kondisi** | **Hasil** |
|---|---|---|
| Topologi | Cisco 1941 | Infrastruktur berjalan normal |
| Keamanan | Cisco 5505 ASA | Sudah terkonfigurasi dan berfungsi baik dalam memblokir akses tidak sah. |
| Pengalamatan IP | DHCP | Tidak terdokumentasi dengan baik |
| Backup ISP | Belum ada | Rentan terhadap *downtime* provider tersebut |

Evaluasi menunjukkan bahwa komponen penting seperti DHCP, *Virtual Local Area Network* (VLAN), *firewall*, dan manajemen *Access Point* telah berfungsi optimal. Kelemahan utama terletak pada topologi fisik (terlihat pada Gambar 1) yang sangat bergantung pada satu *Internet Service Provider* (ISP) tunggal, yakni Gisaka, tanpa adanya jalur cadangan. Hal ini memicu kerentanan sistem terhadap *downtime* apabila penyedia layanan tersebut mengalami gangguan. Ketiadaan diversifikasi rute semacam ini menciptakan titik kegagalan Tunggal (*single point of failure*) yang berpotensi melumpuhkan total operasional layanan, kondisi yang dapat diantisipasi melalui penerapan redudansi untuk menyediakan jalur alternatif secara otomatis [9].

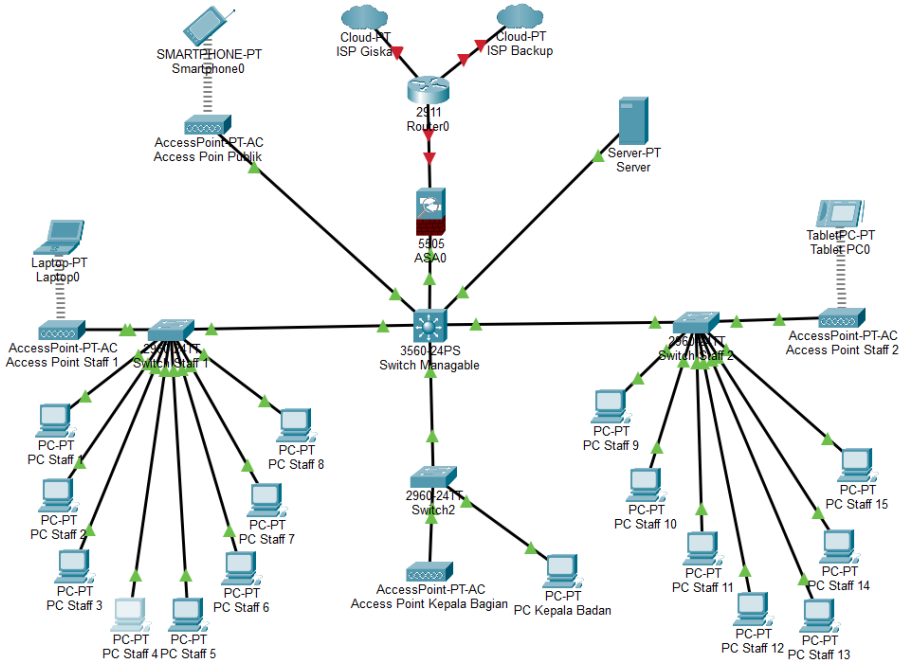
**TeknoIS: Jurnal Ilmiah Teknologi Informasi dan Sains**
Volume 16 Number 2, July 2026 Page. 215-223
Journal Homepage: https://teknois.unbin.ac.id/index.php/JBS/
Received: April 2026; Accepted: July 2026; Published: July 2026



Gambar 1. Topologi Jaringan Eksisting Bapenda Majalengka

## DESAIN ARSITEKTUR REKOMENDASI

Berdasarkan hasil analisis kesenjangan pada fase sebelumnya, rancangan perbaikan pada fase *Design* difokuskan untuk mengatasi kelemahan ketiadaan redundansi koneksi. Tanpa merombak struktur jaringan dasar secara signifikan, desain usulan menambahkan satu jalur koneksi baru yang difungsikan sebagai ISP cadangan (*backup*). Topologi usulan ini divisualisasikan pada Gambar 2.



Gambar 2. Topologi Jaringan Usulan dengan Redundansi ISP

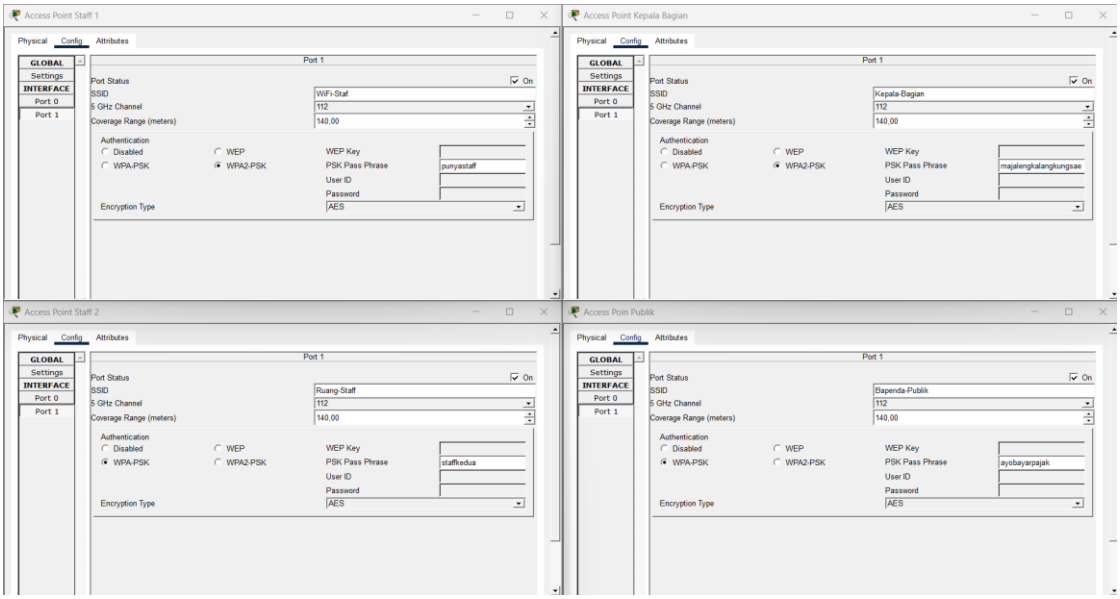
**TeknoIS: Jurnal Ilmiah Teknologi Informasi dan Sains**
Volume 16 Number 2, July 2026 Page. 215-223
Journal Homepage: https://teknois.unbin.ac.id/index.php/JBS/
Received: April 2026; Accepted: July 2026; Published: July 2026

Penambahan jalur cadangan ini dirancang agar *router* dapat diatur untuk melakukan *failover* (perpindahan koneksi secara otomatis) dan berpotensi untuk dioptimalkan lebih lanjut menggunakan mekanisme distribusi beban (*load balancing*) dengan metode *Per Connection Classifier* (PCC). Integrasi *failover* dengan algoritma PCC ini secara akademis telah terbukti efektif dalam membagi dan menyeimbangkan beban arus data antar ISP, sehingga stabilitas performa jaringan dan parameter kualitas layanan (*Quality of Service*) tetap terjamin optimal bahkan saat sistem dihadapkan pada lalu lintas akses yang padat [10].

## 2. PEMBAHASAN

### IMPLEMENTASI JARINGAN SECARA VIRTUAL

Mengingat operasional instansi pemerintah membutuhkan kondisi *zero downtime*, fase implementasi dari desain usulan dieksekusi secara virtual menggunakan perangkat lunak *Cisco Packet Tracer*. Tahap ini mencakup penerapan manajemen hak akses nirkabel dan penulisan skrip perutean pada perangkat *router*. Untuk keamanan *wireless*, akses dibedakan berdasarkan tingkat pengguna (staf, kepala bagian, dan publik) menggunakan parameter *Service Set Identifier* (SSID) dan enkripsi WPA2-PSK yang disesuaikan, sebagaimana ditunjukkan pada Gambar 3.




Gambar 3. Konfigurasi Manajemen Hak Akses Nirkabel

Inti dari fase implementasi ini adalah mengaktifkan mekanisme redundansi. Konfigurasi *failover* diterapkan menggunakan fitur *IP Service Level Agreement* (IP SLA) pada sistem operasi *Cisco* untuk melacak ketersediaan koneksi internet.

### PENGUJIAN DAN OPERASIONAL

Skrip pada tahap implementasi berfungsi agar *router* secara berkelanjutan mengirimkan paket *Internet Control Message Protocol* (ICMP) *echo* untuk memeriksa status jalur ISP utama. Validasi fungsionalitas desain ini diuji melalui beberapa skenario operasional yang hasilnya dirangkum pada Tabel 3.

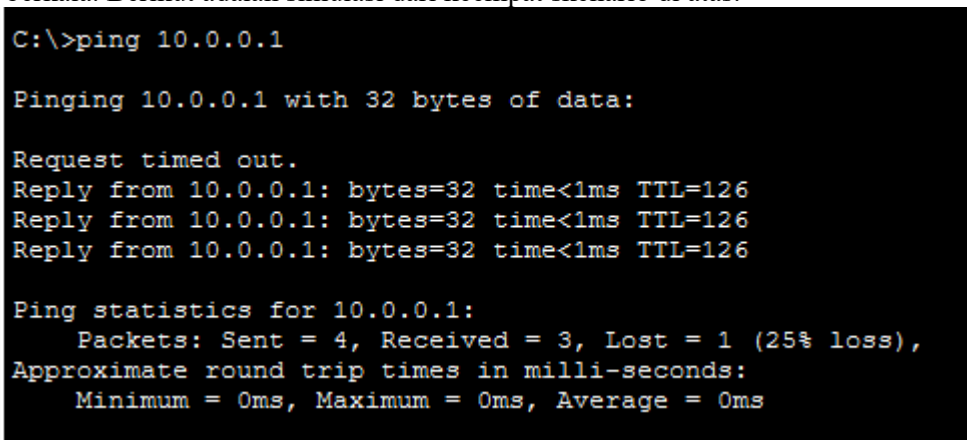
Tabel 3. Skenario Simulasi Pengujian Jaringan

| **Skenario** | **Keterangan** | **Hasil yang diharapkan** |
|---|---|---|
| Kondisi Normal | PC Staf mengakses internet | Koneksi melalui ISP Gisaka |

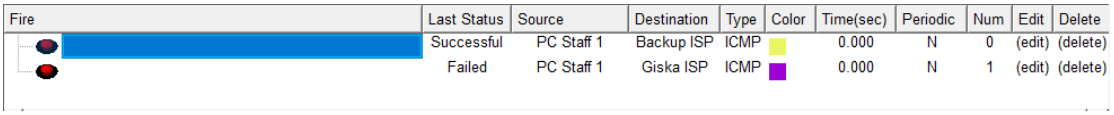
**TeknoIS: Jurnal Ilmiah Teknologi Informasi dan Sains**
Volume 16 Number 2, July 2026 Page. 215-223
Journal Homepage: https://teknois.unbin.ac.id/index.php/JBS/
Received: April 2026; Accepted: July 2026; Published: July 2026

| Skenario | Keterangan | Hasil yang diharapkan |
|---|---|---|
| *Failover* | Memutus koneksi ke ISP Gisaka | *Traffic* otomatis beralih ke ISP *Backup* |
| Pemulihan | Menyambungkan kembali ISP Gisaka | *Traffic* kembali ke ISP utama |
| Keamanan | PC Tamu mencoba mengakses NAS | Tidak berhasil (diblokir VLAN) |

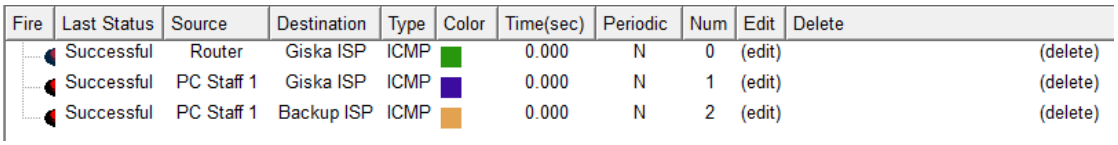
Hasil simulasi membuktikan bahwa rancangan berfungsi secara efektif. Saat koneksi ISP utama disimulasikan terputus, rute data secara otomatis beralih (*failover*) ke antarmuka *GigabitEthernet0/1* (ISP *Backup*), dan kembali ke jalur utama saat koneksi pulih. Selain simulasi teknis, pihak Bapenda Majalengka juga direkomendasikan untuk melakukan pemantauan jaringan secara *real-time* menggunakan perangkat lunak pihak ketiga seperti Zabbix, serta melakukan pengecekan kesehatan perangkat keras dan dokumentasi log kegagalan secara berkala. Berikut adalah simulasi dari keempat skenario di atas.



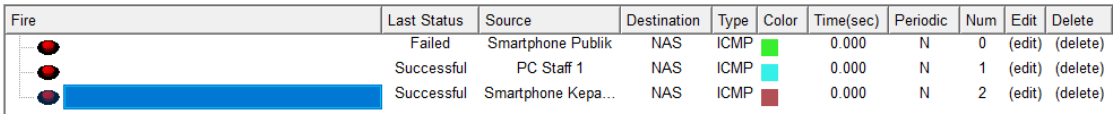

Gambar 4. Simulasi Kondisi Normal




Gambar 5. Simulasi *Failover*




Gambar 6. Simulasi Pemilihan




Gambar 7. Simulasi Keamanan NAS

## REKOMENDASI OPTIMASI LANJUTAN

Sebagai langkah terakhir dari siklus PPDIOO, rekomendasi perbaikan proaktif disusun untuk menjaga performa jaringan Bapenda di masa mendatang seiring dengan bertambahnya beban layanan. Rekomendasi optimasi tersebut disajikan pada Tabel 4.

Tabel 4. Rekomendasi Optimasi Lanjutan

| **Aspek** | **Rekomendasi** |
|---|---|
| Keamanan | Upgrade autentikasi Access Point dari WPA2 ke WPA3 (jika perangkat mendukung) |
| Kinerja | Implementasi QoS untuk memprioritaskan traffic aplikasi perpajakan (SIMPEL PBB, QRIS) |
| Kapasitas | Evaluasi berkala penggunaan *bandwidth* |
| Dokumentasi | Pembuatan peta jaringan terdokumentasi dan skema pengalamatan IP |
| Redundansi | Jika anggaran memungkinkan, tambahkan switch core kedua untuk menghindari *single point of failure* |

Untuk mengatasi tantangan lalu lintas data aplikasi yang semakin padat, implementasi *Quality of Service* (QoS) menjadi kebutuhan prioritas untuk memastikan sistem perpajakan tidak mengalami latensi. Dari sisi keamanan akses, direkomendasikan pembaruan sistem enkripsi ke versi WPA3 jika perangkat keras memungkinkan. Secara keseluruhan, desain arsitektur yang dikembangkan melalui metode PPDIOO ini tidak hanya menyelesaikan persoalan keterbatasan jalur internet yang ada, namun juga merumuskan fondasi infrastruktur digital yang lebih tangguh dan aman bagi operasional Bapenda Kabupaten Majalengka.

## D. KESIMPULAN

Infrastruktur jaringan pada Badan Pendapatan Daerah Kabupaten Majalengka secara fungsional telah memiliki fondasi yang kuat dengan penerapan segmentasi logis melalui VLAN, otomasi pengalamatan IP menggunakan DHCP, serta sistem penyimpanan data terpusat menggunakan NAS Synology. Namun, hasil evaluasi mengidentifikasi adanya titik kritis pada ketersediaan layanan akibat ketergantungan penuh pada satu penyedia layanan internet (ISP) tunggal, yakni Gisaka, yang menyebabkan risiko *downtime* tinggi apabila terjadi gangguan teknis pada jalur utama tersebut.

Penerapan metodologi PPDIOO dalam penelitian ini berhasil merumuskan solusi strategis berupa desain arsitektur jaringan yang mendukung redundansi melalui penambahan ISP *backup* dan konfigurasi mekanisme *failover* otomatis pada *router*. Melalui pengujian simulasi pada *Cisco Packet Tracer*, desain usulan ini terbukti mampu menjaga kontinuitas layanan digital perpajakan daerah, di mana paket data secara otomatis dialihkan ke jalur cadangan saat koneksi utama terputus tanpa mengganggu aksesibilitas sistem.

Sebagai langkah optimasi jangka panjang untuk mendukung ekosistem *e-government* yang lebih tangguh, disarankan bagi pihak Bapenda Majalengka untuk mengimplementasikan kebijakan *Quality of Service* (QoS) guna memprioritaskan lalu lintas data aplikasi krusial seperti SIMPEL PBB dan QRIS. Selain itu, pembaruan standar keamanan nirkabel ke versi WPA3 dan penambahan perangkat *switch core* cadangan sangat direkomendasikan untuk menghilangkan potensi *single point of failure* pada tingkat perangkat keras demi menjamin ketersediaan layanan publik yang stabil dan aman.

## E. DAFTAR PUSTAKA

[1] R. A. Octaviyani dan B. Soewito, "Perancangan Ulang Topologi Jaringan Dengan Kerangka Kerja Ppdioo," *Teknologi*, vol. 13, no. 1, hal. 34–41, 2023.

[2] Viky G.L. Radja Pono, Indah Octaviani Laleb, dan Demas Eklopas Neno, "Implementasi Quality of Service (QoS) pada Jaringan Intra Pemerintah," *J. Teknol. dan Manaj. Ind. Terap.*, vol. 4, no. I, hal. 97–103, 2025, doi: 10.55826/jtmit.v4ii.789.

[3] H. P. Fitrian, T. S. Latifah, M. Imroatuddin, I. A. Maulana, dan F. A. Al Anshari, "Analisis Performa Topologi Star Dan Mesh Dalam Implementasi Jaringan Lan Pada Lingkungan Perkantoran," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 9, no. 1, hal. 1399–1403, 2025, doi: 10.36040/jati.v9i1.12539.

[4] E. D. Sitanggang, Misdem Sembiring, dan Beny Irawan, "Pengembangan Layanan Pemblokiran Situs Bermuatan Negatif menggunakan DNS Sinkhole dan Layanan DNS Quad 9 dengan Metode PPDIOO," *LOFIAN J. Teknol. Inf. dan Komun.*, vol. 3, no. 2, hal. 16–24, 2024, doi: 10.58918/lofian.v3i2.240.

[5] D. Auzini Yasmine dan A. Nurliana Putri, "Analisis Dan Desain Jaringan Vlsm Pada Smait Al-Uswah Surabaya," *J. Teknol. Inf.*, vol. 4, no. 2, hal. 577–585, 2023, doi: 10.46576/djtechno.

[6] A. I. Haris, B. Riyanto, F. Surachman, dan A. A. Ramadhan, "Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi," *Komputika J. Sist. Komput.*, vol. 11, no. 1, hal. 67–76, 2022, doi: 10.34010/komputika.v11i1.5227.

[7] G. A. P. F. A. N. Agussalim, "Desain dan Manajemen Jaringan MTsN Kota Madiun Menggunakan Cisco Packet Tracer dengan Metode PPDIOO" J. Ilmu Tek., Vol.1, no. 2, hal. 298-306, 2024, [daring]. Tersedia pada: https://doi.org/10.62017/tektonik

[8] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*, 3 ed. Bandung: Alfabeta, 2021.

[9] A. Octavian dan G. Purnama, "Redudancy Dengan Intervlan Routing pada Pln Uid" JTET (Jurnal Inform. dan Tek. Elektro Ter., Vol.12 No.2, 2924

[10] M. F. Darmawan dan S. Risnanto, "Implementasi Failover Gateway Recursive Dan Load Balancing Menggunakan Metode Per Connection Classifier" Infotronik J.Teknol. Inf. Dan Elektron., Vol. 8, No.2, hal 56, 2023, doi: 10.32897/infotronik.2023.8.2.1887.