Jurnal Teknlogi Informatika dan Komputer MH. Thamrin p-ISSN 2656-9957; e-ISSN 2622-8475
Volume 12 No 2; September 2026 Hal 1157-1175

Implementation of a MikroTik-Based PPPoE Protocol for Authentication and Access Security in RT/RW-Net

Agus Widaksono [1)*)], Sri Lestanti [2)], Filda Febrinita [3)]

[1)2)3)]Teknik Informatika, Fakultas Teknik dan Informatika, Universitas Islam Blitar
[*)]**Correspondence author**: aguswidaksono4@gmail.com, Blitar, Indonesia
DOI: https://doi.org/10.37012/jtik.v12i2.3549

Abstract

The RT/RW-Net ADC-Net network in Suruhwadang Village with more than 300 customers faces connection instability and security vulnerabilities due to conventional static IP management on a flat network architecture. This research aims to design and implement a MikroTik-based PPPoE network to provide a centralized authentication system and client isolation using the Network Development Life Cycle (NDLC) method. The functional evaluation of the system is tested through Black Box Testing. The test results of 3 clients through 9 test scenarios recorded 100% absolute success. The client isolation feature has been proven to be effective in mitigating local cyberattacks such as ARP Spoofing and NetCut through blocking communication between users with a 100% Request Timed Out (RTO) status. The dynamic Simple Queue feature is precisely able to distribute bandwidth according to regular (5Mbps), gaming (10Mbps), and premium (20Mbps) service packages. In addition to improving stability and security, the system delivers massive operational efficiencies for administrators by cutting activation procedures from 4 manual stages to 2 automatic. In conclusion, the MikroTik-based PPPoE protocol is effective and feasible to be used as a standard for centralized communal network governance.

Keywords: *PPPoE, MikroTik, RT/RW-Net, NDLC, Flat Network Management*

Abstrak

Jaringan RT/RW-Net ADC-Net di Desa Suruhwadang dengan lebih dari 300 pelanggan menghadapi ketidakstabilan koneksi dan kerentanan keamanan akibat manajemen IP Statis konvensional pada arsitektur *flat network*. Penelitian ini bertujuan merancang dan mengimplementasikan jaringan PPPoE berbasis *MikroTik* untuk menyediakan sistem autentikasi terpusat dan isolasi klien menggunakan metode *Network Development Life Cycle* (NDLC). Evaluasi fungsional sistem diuji melalui *Black Box Testing*. Hasil pengujian terhadap 3 klien melalui 9 skenario uji mencatatkan keberhasilan mutlak 100%. Fitur isolasi klien terbukti efektif memitigasi serangan siber lokal seperti ARP *Spoofing* dan *NetCut* melalui pemblokiran komunikasi antar-pengguna dengan status *Request Timed Out* (RTO) 100%. Fitur *Simple Queue* dinamis secara presisi mampu mendistribusikan *bandwidth* sesuai paket layanan reguler (5Mbps), *game* (10Mbps), dan premium (20Mbps). Selain meningkatkan stabilitas dan keamanan, sistem ini menghadirkan efektifitas operasional masif bagi administrator dengan memangkas prosedur aktivasi dari 4 tahapan manual menjadi 2 tahapan otomatis, serta mempercepat waktu konfigurasi per *user*. Kesimpulannya, protokol PPPoE berbasis *MikroTik* efektif dan layak digunakan sebagai standar tata kelola jaringan komunal secara terpusat.

Kata Kunci: PPPoE, *MikroTik*, RT/RW-*Net*, NDLC, Manajemen *Flat Network*

PENDAHULUAN

Di era transformasi digital global yang berkembang pesat, akses internet telah bertransformasi dari sekadar teknologi pelengkap menjadi kebutuhan primer yang mendasari berbagai aktivitas peradaban manusia modern (Arbi & Amrullah, 2024). Ketergantungan terhadap konektivitas digital ini tidak hanya dirasakan oleh sektor makro seperti korporasi dan pemerintahan, tetapi juga meresap kuat ke dalam unit sosial terkecil yaitu skala rumah tangga. Jaringan internet kini memegang peranan krusial sebagai infrastruktur utama yang menopang kegiatan masyarakat dunia, mulai dari pendidikan, bisnis, komunikasi, hingga akses informasi tanpa batas (Bumbungan, 2025), (Tazak'ka & Sofyan, 2025). Pertumbuhan eksponensial pengguna internet global ini menuntut adanya ketersediaan koneksi yang tidak hanya sekadar cepat, melainkan juga stabil, aman, dan mudah diakses oleh seluruh lapisan masyarakat secara merata. Oleh karena itu, pemerataan akses digital menjadi agenda penting bagi institusi internasional demi memastikan tidak ada kelompok masyarakat yang tertinggal dalam pusaran kemajuan teknologi informasi masa kini (Sugari & Hilalludin, 2025).

Di tingkat nasional, fenomena adopsi digital ini juga tercermin secara nyata melalui tingginya angka penetrasi penggunaan internet di seluruh wilayah Indonesia. Laporan terbaru dari Asosiasi Penyelenggara Jasa Internet Indonesia mencatat bahwa tingkat penetrasi internet nasional telah mencapai persentase yang sangat dominan dari total populasi penduduk. Meskipun statistik nasional tersebut menunjukkan tren pertumbuhan yang sangat positif, realitas empiris di lapangan masih menyisakan tantangan besar berupa kesenjangan akses infrastruktur telekomunikasi di berbagai daerah pinggiran (Setyawan dkk., 2025). Ketimpangan akses ini diyakini sangat dipengaruhi oleh biaya berlangganan dari penyedia layanan komersial berskala besar yang dirasa masih terlalu membebani kemampuan finansial masyarakat menengah ke bawah (Kurniawan, 2025). Akibatnya, banyak warga terpaksa beralih pada konektivitas seluler alternatif walaupun kualitas sinyalnya sering kali tidak menentu dan sangat dibatasi oleh mekanisme pembagian sistem kuota penggunaan wajar.

Guna menjembatani ketimpangan akses digital dan hambatan tarif dari penyedia besar, masyarakat di berbagai kawasan perumahan mulai membangun jaringan internet lokal secara mandiri yang sering dikenal dengan istilah RT/RW-Net. Model penyediaan internet berbasis komunitas gotong royong ini hadir sebagai solusi praktis yang menawarkan koneksi dengan tarif jauh lebih ekonomis dan metode distribusi yang sangat fleksibel bagi lingkungan setempat. Implementasi nyata dari sistem jaringan swadaya masyarakat tersebut saat ini

dapat diamati langsung pada operasional layanan ADC-Net yang berkedudukan di Desa Suruhwadang, Kecamatan Kademangan, Kabupaten Blitar. Jaringan penyedia konektivitas lokal ini diketahui telah berkembang secara masif dan mengambil peran penting dalam melayani kebutuhan akses internet bagi lebih dari tiga ratus pelanggan aktif setiap harinya. Namun, seiring dengan penambahan beban jumlah pelanggan yang besar, infrastruktur ini mulai membutuhkan mekanisme pengelolaan terstruktur agar kualitas layanannya tetap memenuhi standar keamanan maupun kenyamanan penggunanya(Husaini & Sari, 2023).

Berbagai kendala operasional yang serius mulai sering terjadi akibat model pengelolaan utama pada jaringan ADC-Net saat ini masih bergantung penuh pada arsitektur jaringan datar konvensional dengan manajemen alamat jaringan yang statis. Pendekatan sistem yang sangat terbuka dan tanpa melalui tahapan autentikasi wajib ini mengakibatkan pengelola jaringan sangat kesulitan dalam mendeteksi atau membedakan perangkat pengguna yang memiliki hak akses resmi. Akibat lemahnya kontrol tersebut, ketiadaan proses isolasi perlindungan antar-klien membuat struktur jaringan lokal ini menjadi sangat rawan diretas melalui metode manipulasi jaringan tingkat dasar seperti serangan pemalsuan *Address Resolution Protocol* atau ARP *Spoofing* (Nursobah dkk., 2023). Pada sisi pemeliharaan kualitas koneksi, metode pembagian kecepatan lalu lintas data yang masih dikerjakan secara manual turut memicu ketidakadilan distribusi yang mengakibatkan koneksi menjadi sangat melambat saat jam operasional puncak (Sari dkk., 2024). Masalah integritas keamanan data dan tidak efektifnya tata kelola alokasi jaringan lokal ini dipercaya akan terus menimbulkan kerugian teknis apabila tidak dimitigasi secepatnya menggunakan pembaruan konfigurasi yang lebih mutakhir(Firmansyah dkk., 2025).

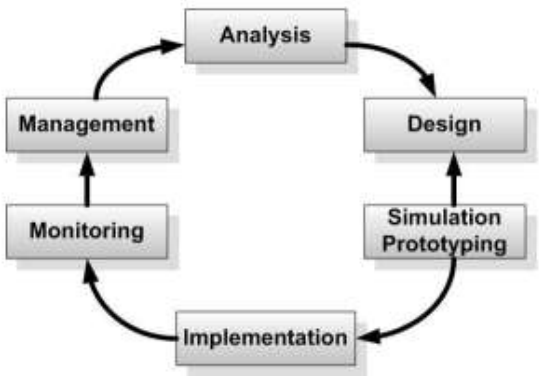
Merespons urgensi permasalahan stabilitas dan tingginya tingkat kerentanan tersebut, penerapan pembaruan teknologi *Point-to-Point Protocol over Ethernet* (PPPoE) dengan mengandalkan mesin peladen *router* pusat menjadi rekomendasi penyelesaian yang sangat tepat sasaran. Inovasi protokol keamanan jaringan terpusat ini memiliki mekanisme khusus untuk merombak lalu lintas terbuka menjadi sebuah jalur transmisi privat yang selalu menuntut penggunanya memasukkan data kredensial sandi sebelum bisa terhubung. Penerapan kapabilitas sistem perlindungan baru ini akan memudahkan administrator dalam memblokir jalur interaksi antar-pengguna, sehingga mampu secara drastis menekan seluruh potensi kejahatan internal di ruang lingkup jaringan komunitas lokal. Selain keunggulan proteksi keamanan, integrasi fitur bawaan pada peranti penyedia layanan ini juga secara otomatis mampu menjalankan perintah manajemen pembatasan lalu lintas koneksi secara

lebih adil dan merata per pelanggan (Hasany & Setiawan, 2025), (Fadilah dkk., 2025), (Samad dkk., 2025). Berdasarkan seluruh pertimbangan tersebut, pelaksanaan penelitian ini dipandang sangat esensial untuk segera direalisasikan demi menghasilkan desain operasional internet komunal yang jauh lebih stabil, terstruktur pengelolaannya, dan terlindungi secara sempurna.

METODE PENELITIAN

Penelitian ini dirancang secara sistematis guna menyelesaikan kendala teknis pada infrastruktur jaringan internet komunitas melalui penyelesaian yang dapat diterapkan secara langsung. Secara keseluruhan, studi ini diklasifikasikan sebagai Penelitian Terapan atau *Applied Research* karena bertujuan untuk mengimplementasikan teknologi dalam memecahkan problematika operasional secara praktis di lapangan, bukan sekadar merumuskan atau memvalidasi teori baru. Adapun lokasi pelaksanaannya difokuskan pada infrastruktur milik mitra, yaitu jaringan ADC-Net yang berkedudukan di Desa Suruhwadang RT 02 RW 07, Kecamatan Kademangan, Kabupaten Blitar. Serangkaian proses perancangan, implementasi, hingga tahap evaluasi akhir ini diselenggarakan dalam rentang waktu pelaksanaan selama 6 (enam) bulan, yang dimulai sejak November 2025 hingga Juli 2026.

Mengingat riset ini berorientasi pada pengembangan sekaligus perbaikan sistem jaringan yang tengah beroperasi, kerangka kerja rekayasa yang diadopsi adalah *Network Development Life Cycle* (NDLC). Metodologi khusus arsitektur jaringan ini dipilih lantaran memiliki karakteristik siklus yang sistematis, terukur, dan memfasilitasi perbaikan yang berkesinambungan tanpa mengganggu layanan pengguna aktif.



Gambar 1. Tahapan NDLC

Pendekatan pengembangan ini dieksekusi secara mengalir melalui enam fase berurutan yang menaungi seluruh aktivitas penelitian (Prayitno & Yasir, 2025), (Prasetyo dkk., 2025).

1. *Analysis*: Tahapan awal yang bertujuan untuk mengidentifikasi berbagai kebutuhan teknis sistem dan jaringan.
2. *Design*: Tahapan pembuatan desain atau perancangan topologi jaringan, baik secara logis maupun fisik.
3. *Simulation*: Tahapan pengujian terhadap desain sistem yang telah dibuat melalui pengujian di ruang terbatas.
4. *Implementation*: Tahapan penerapan atau instalasi konfigurasi secara langsung pada perangkat keras utama, lalu diakhiri dengan pengujian sistem menggunakan *blackbox testing* serta dilanjutkan dengan validasi ahli.
5. *Monitoring*: Tahapan pemantauan dan pengawasan terhadap kinerja sistem setelah diimplementasikan.
6. *Management*: Tahapan akhir yang berfokus pada pemeliharaan dan tata kelola jaringan secara jangka panjang.

Penelitian ini menggunakan pendekatan triangulasi data untuk memastikan keakuratan informasi melalui empat tahapan utama:

1. Observasi: Mengamati langsung topologi fisik, spesifikasi perangkat, dan celah keamanan jaringan yang sedang berjalan.
2. Wawancara: Melakukan tanya jawab semi-terstruktur dengan pemilik dan teknisi terkait kendala operasional sehari-hari.
3. Studi Literatur: Mengkaji jurnal ilmiah dan dokumentasi standar jaringan sebagai landasan teori.
4. Instrumen Pengujian: Menggunakan lembar catatan khusus untuk merekam hasil pengujian sistem secara terstruktur.

Untuk mendukung simulasi dan implementasi, penelitian ini membutuhkan perangkat keras dan perangkat lunak sebagai berikut:

1. Perangkat Keras:
   a. *MikroTik RouterBoard* RB951G-2HnD (sebagai router utama dan *server* autentikasi).
   b. *Router wireless* (Tenda N301 atau TP-*Link* WR840N) untuk simulasi penerima (*client*).

c. Laptop (minimal *prosesor Core* i3/i5, RAM 8GB) untuk stasiun kerja administrator.
d. Gawai *Android* dan kabel LAN UTP Cat5e.

2. Perangkat Lunak:
   a. Sistem Operasi *MikroTik Router* OS versi 6.48.
   b. Aplikasi manajemen *Winbox* versi 3.38.
   c. Perangkat lunak diagnosis: *Advanced* IP *Scanner* dan *Speedtest by* Ookla.
   d. Perangkat lunak pemodelan: *Cisco Packet Tracer* dan *Microsoft Visio*.

HASIL DAN PEMBAHASAN

Hasil transformasi jaringan ADC-Net menuju sistem PPPoE menggunakan metode NDLC diuraikan sebagai berikut:

1. Tahap *Analysis*

Tahap analisis dilakukan melalui observasi lapangan, wawancara dengan pihak pengelola, dan studi literatur untuk mengidentifikasi kondisi aktual jaringan di ADC-Net, Desa Suruhwadang. Berdasarkan evaluasi eksisting, infrastruktur jaringan tersebut masih menerapkan konsep *flat network* dengan metode alokasi IP statis dan belum memiliki mekanisme autentikasi pengguna. Ketiadaan sistem validasi ini memungkinkan setiap perangkat pelanggan terhubung secara langsung ke jaringan tanpa pengawasan, yang pada akhirnya menyulitkan administrator dalam mengontrol identitas pengguna yang aktif dan melakukan tata kelola secara terpusat. Selain itu, seluruh pelanggan yang dibiarkan berada dalam satu segmen jaringan yang sama telah memicu tingginya risiko keamanan siber, terutama kerentanan terhadap serangan manipulasi seperti ARP *Spoofing*.

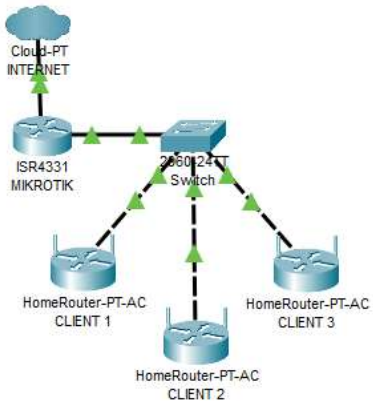
Dampak lanjutan dari model pengelolaan yang masih berjalan manual ini adalah seringnya terjadi ketidakseimbangan distribusi lalu lintas data antar-pelanggan. Hal ini berujung pada keluhan terkait koneksi internet yang tidak stabil dan penurunan performa secara drastis pada jam-jam sibuk. Untuk mengatasi berbagai kendala teknis dan manajerial tersebut, penerapan *Point-to-Point Protocol over Ethernet* (PPPoE) menggunakan peranti *router* MikroTik direkomendasikan sebagai solusi utama. Pendekatan ini dipilih karena protokol PPPoE dinilai sangat efektif untuk diterapkan pada jaringan RT/RW-Net dalam menyediakan fungsi autentikasi identitas berbasis *username* dan *password*, mengotomatisasi manajemen batas kecepatan, serta

memperketat keamanan akses secara terpusat tanpa memerlukan tambahan perangkat *server*.

2. *Design*

a. Perancangan Topologi

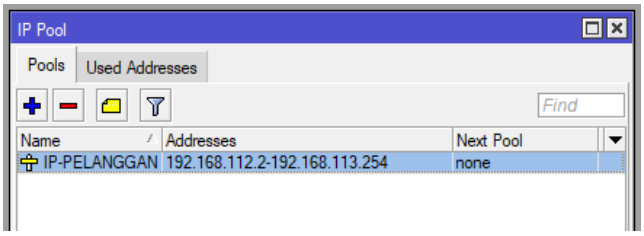
Tahap perancangan solusi teknis ini mengadopsi arsitektur *tree topology* dengan menempatkan *router MikroTik* sebagai pusat kontrol yang menghubungkan sumber internet ISP dengan seluruh klien. Seperti yang diilustrasikan pada Gambar 1, aliran koneksi internet dari penyedia layanan diteruskan ke *router MikroTik* yang bertindak sebagai PPPoE *Server* untuk mengelola autentikasi, kemudian didistribusikan melalui perangkat *switch hub* menuju tiga unit *Home Router* di sisi pelanggan.



Gambar 2. Rancangan Topologi Jaringan

b. Perancangan Pengalamatan IP

Sistem pengalamatan logis pada jaringan dirancang dengan mengonfigurasi IP *Pool* pada rentang alamat 192.168.112.2 hingga 192.168.113.254 guna mengisolasi segmen manajemen dan segmen pelanggan demi meningkatkan faktor keamanan. Skema pengalamatan dinamis tersebut secara terstruktur disajikan pada Gambar 3 yang mengilustrasikan pembagian blok IP berdasarkan profil autentikasi masing-masing pengguna.



Gambar 3. Pembuatan IP *Pool*

c. Perancangan Manajemen *Flat Network*

Perancangan tata kelola lini digital ini berfokus pada minimalisasi ketimpangan trafik melalui otomatisasi fitur *Simple Queue* yang diintegrasikan langsung pada menu PPP *Profile* di *router MikroTik*. Kebijakan pembatasan kecepatan ini dibagi secara terstruktur ke dalam tiga kategori paket komersial, meliputi paket reguler dengan kapasitas 5Mbps, paket *game* sebesar 10Mbps, dan paket *premium* hingga 20Mbps.

3. Tahap *Simulation*

Setelah perangkat keras siap, susunan simulasi hubungan fisik, alur data, dan pengabelan ditunjukkan pada Gambar 4:

Gambar 4. Simulasi Jaringan

Guna menghindari gangguan pada jaringan aktif ADC-Net, simulasi terbatas dilakukan menggunakan satu unit MikroTik RB951G-2HnD dan tiga *wireless router* klien. Hasil simulasi membuktikan bahwa protokol PPPoE sukses menangani proses *dial-up* secara simultan sekaligus membentuk aturan *Simple Queue* dinamis secara otomatis, sehingga menjamin konfigurasi aman dari potensi konflik sebelum benar-benar diterapkan pada jaringan produksi.

4. Tahap *Implementation*

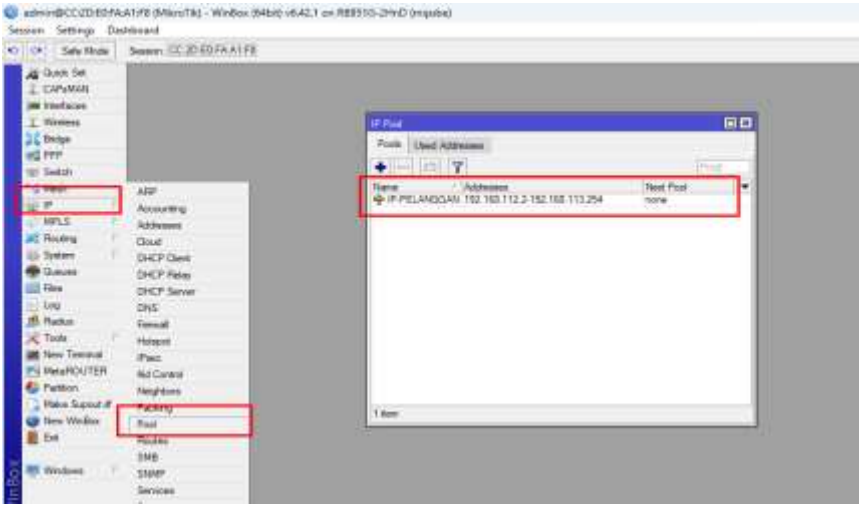
Tahap implementasi mengeksekusi rancangan menggunakan *Winbox MikroTik* dengan dua konfigurasi utama yaitu *server* dan *client* lalu diakhiri dengan pengujian *blackbox* dan validasi ahli.

a. Implementasi Sisi Server (*Mikrotik*)

Pada sisi *server*, langkah teknis konfigurasi *MikroTik* untuk menangani permintaan PPPoE pelanggan adalah sebagai berikut:

1) Pembuatan IP-*Pool*

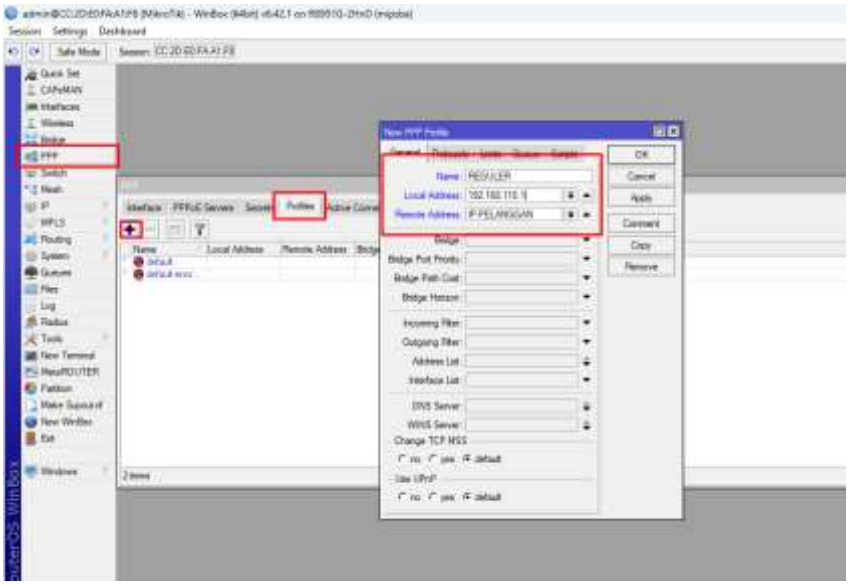
Gambar 5 menunjukkan pembuatan rentang IP dinamis (IP *Pool*) khusus pelanggan untuk mencegah bentrokan alamat IP di jaringan ADC-Net.



Gambar 5. Konfigurasi IP *Pool*

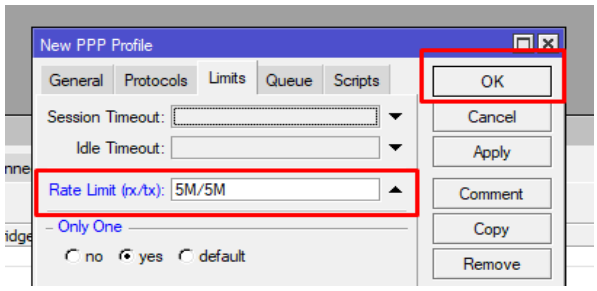
2) Pembuatan PPP *Profiles*

Gambar 6 menampilkan pembuatan profil pelanggan yang berfungsi mengatur limitasi *bandwidth* secara otomatis dan mengikatnya dengan IP *Pool*.



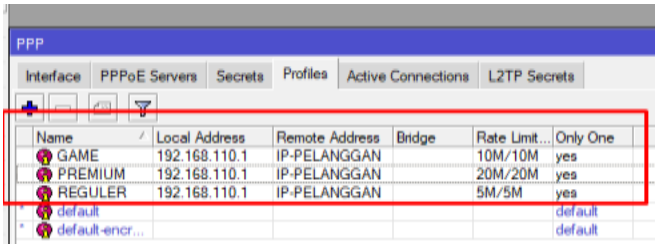
Gambar 6. Konfigurasi PPP *Profile*

Gambar 7 mengilustrasikan pengaktifan layanan PPPoE *Server* pada *interface* MikroTik agar *router* utama dapat menerima permintaan *dial-up* dari peranti klien.



Gambar 7. Limit Kecepatan pada Masing-Masing Profil

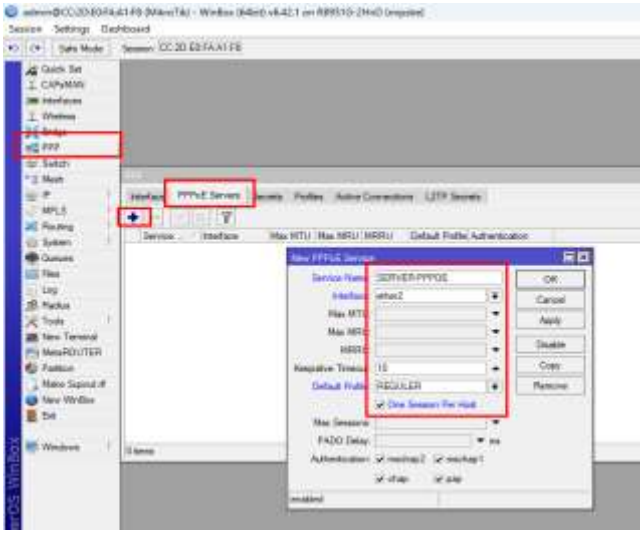
Gambar 8 memperlihatkan pembuatan *username* dan *password* unik bagi setiap pelanggan yang dihubungkan dengan profil paket internet mereka.



Gambar 8. Seluruh Profil Ketika Selesai Dibuat

3) Konfigurasi PPPoE *Server*

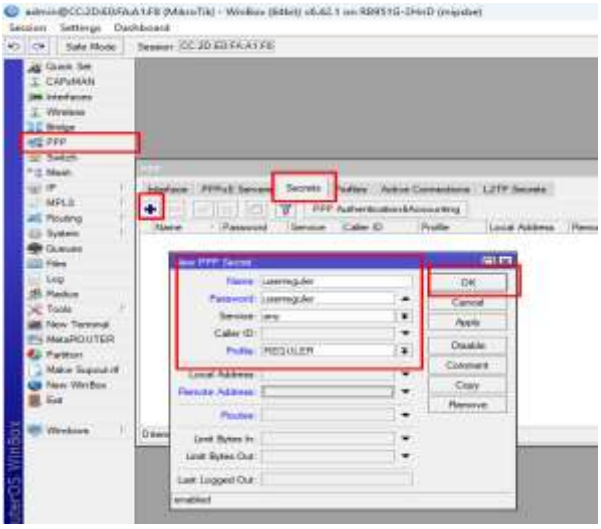
Gambar 9 menunjukkan tahap pengisian akun kredensial pada *Wireless Router* warga untuk mengubah metode akses menjadi berbasis sesi *dial-up*.



Gambar 9. Konfigurasi PPPoE *Server*

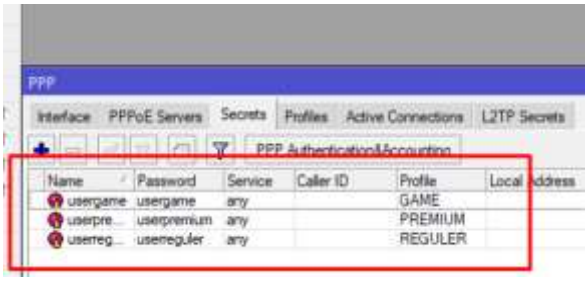
4) Pendaftaran *Database Secrets*

Gambar 10 menampilkan daftar klien yang berhasil *login* ke *server*, lengkap dengan informasi IP dinamis yang didapat dan durasi koneksi aktif mereka.



Gambar 10. Pembuatan *User* dan *Password* PPPoE

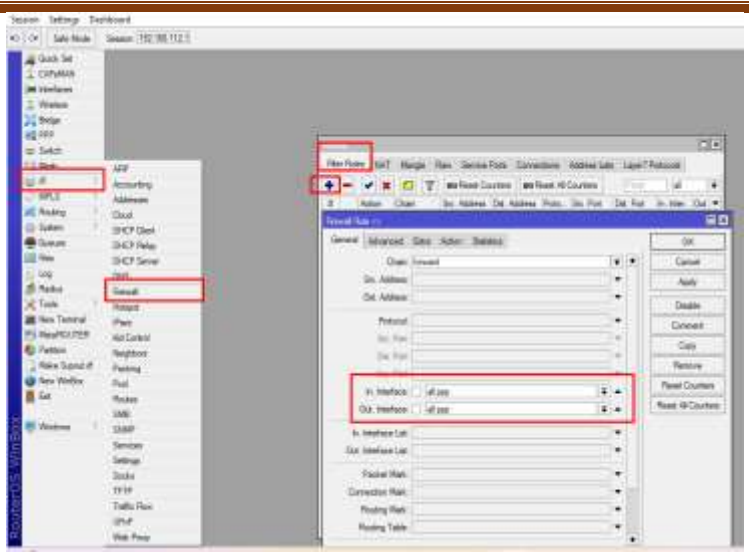
Gambar 11 membuktikan bahwa *router* milik klien telah berhasil mendapatkan jalur akses internet secara penuh setelah proses autentikasi.



Gambar 11. Daftar Pengguna

5) Penerapan *Firewall Filter*

Gambar 12 menunjukkan bahwa peranti klien sukses memperoleh alokasi IP secara otomatis dan dinamis sesuai rentang yang diatur pada *server*.



Gambar 12. Pembuatan *Filter* untuk Mencegah ARP *Spoofing*

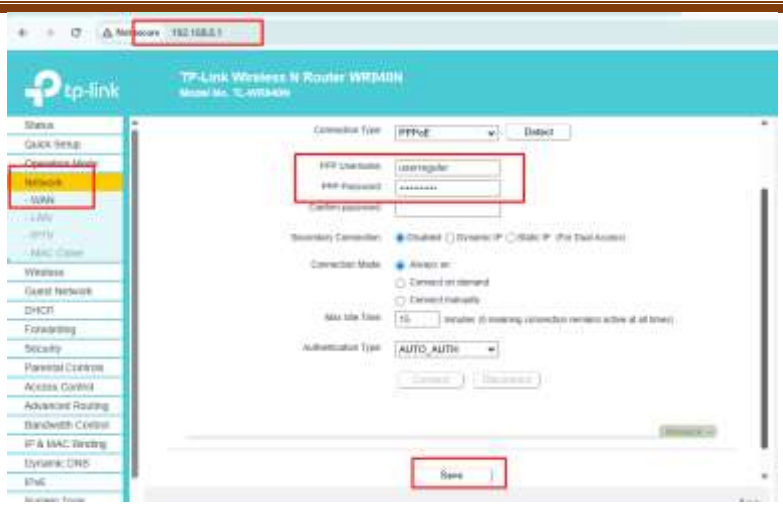
b. Implementasi Sisi *Client* (*Wireless Router*)

Konfigurasi pada sisi klien (*Wireless Router*) untuk mengubah metode akses statis menjadi sesi PPPoE *Client* dilakukan melalui langkah-langkah berikut:

Gambar 13 dibawah membuktikan hasil *speedtest* di sisi klien sudah dibatasi secara presisi sesuai dengan aturan *Simple Queue* pada profil paket yang mereka pilih.

Gambar 13. *Login* Router TP-*Link*

Gambar 14 menegaskan bahwa perangkat antar-klien kini saling terisolasi sehingga aman dari upaya pemindaian ilegal maupun serangan manipulasi jaringan.



Gambar 14. *Setting* PPPoE *Client* pada Router

c. Pengujian Sistem

Tabel berikut menyajikan hasil *Black Box Testing* terhadap 3 perangkat *client*. Pengujian mencakup 9 skenario utama, mulai dari validasi autentikasi, pembatasan kecepatan, hingga isolasi jaringan.

Tabel 1.
Hasil Pengujian *Blackbox*

No	Client ke	Skenario Ke									Hasil Pengujian		Keterangan
		1	2	3	4	5	6	7	8	9	Valid	Tidak Valid	
1	Client ke 1	✓	✓	✓	✓	✓	✓	✓	✓	✓	9		Sistem berjalan sesuai dengan seharusnya
2	Client ke 2	✓	✓	✓	✓	✓	✓	✓	✓	✓	9		Sistem berjalan sesuai dengan seharusnya
3	Client ke 3	✓	✓	✓	✓	✓	✓	✓	✓	✓	9		Sistem berjalan sesuai dengan seharusnya

Proses perhitungan persentase kelayakan pada Tabel 1 adalah sebagai berikut:

$$P = \left(\frac{Skenario\ Berhasil}{Total\ Skenario}\right) x\ 100\%$$

$$P = \left(\frac{27}{27}\right) x\ 100\% = 100\%$$

Berdasarkan pengujian fungsional menggunakan *Black Box Testing*, sistem infrastruktur berbasis PPPoE pada ADC-Net mencatat tingkat keberhasilan 100% tanpa cacat pada 27 percobaan, yang memastikan fitur-fitur krusial seperti autentikasi

login, manajemen *bandwidth* dinamis, dan isolasi keamanan klien berjalan dengan stabil serta layak masuk ke dalam validasi ahli untuk menguji kelayakan operasional sistem yang telah dibuat. Berikut merupakan hasil penilaian validasi ahli pada Tabel 2:

Tabel 2.
Lembar Penilaian Validasi Ahli

Lembar Penilaian Validasi Ahli		
No	**Aspek yang dinilai**	**Penliaian Ahli**
Aspek Kelayakan Desain Sistem		
1	Kesesuaian topologi jaringan dengan kebutuhan penelitian	Topologi jaringan yang dirancang telah sesuai dengan kebutuhan implementasi PPPoE pada jaringan RT/RW-Net dan mendukung proses autentikasi pengguna secara terpusat.
2	Ketepatan penggunaan metode NDLC dalam pengembangan jaringan	Metode NDLC telah diterapkan secara sistematis mulai dari tahap analisis hingga monitoring sehingga proses pengembangan jaringan berjalan terstruktur.
3	Kesesuaian rancangan IP *Address* dengan implementasi jaringan	Pengalamatan IP yang digunakan telah sesuai dengan kebutuhan jaringan dan mendukung konfigurasi PPPoE *Server* dengan baik.
4	Kesesuaian konfigurasi PPPoE dengan tujuan penelitian	Konfigurasi PPPoE telah berjalan sesuai tujuan penelitian dalam meningkatkan autentikasi dan keamanan akses jaringan.
5	Kesesuaian desain *firewall* untuk keamanan jaringan	*Firewall* dan isolasi klien yang diterapkan mampu membantu meningkatkan keamanan jaringan antar pengguna.
Aspek Implementasi Sistem		
1	Ketepatan implementasi autentikasi PPPoE	Sistem autentikasi PPPoE berhasil diterapkan dengan baik dan mampu membatasi akses hanya kepada pengguna terdaftar.
2	Ketepatan implementasi isolasi klien	Implementasi isolasi klien telah berjalan sesuai rancangan dan mampu mengurangi akses langsung antar pengguna jaringan.
3	Ketepatan implementasi manajemen *Flat network*	Pembagian *Flat network* menggunakan PPP *Profile* dan *Simple Queue* telah berjalan sesuai kebutuhan pengguna jaringan.
4	Kesesuaian konfigurasi MikroTik dengan kebutuhan RT/RW-Net	Konfigurasi MikroTik yang diterapkan sudah sesuai dengan kebutuhan pengelolaan jaringan RT/RW-Net skala kecil hingga menengah.
5	Kemudahan monitoring pengguna pada sistem	Sistem mempermudah administrator dalam melakukan monitoring pengguna aktif melalui fitur *Active* PPPoE.
Aspek Pengujian Sistem		
1	Kesesuaian skenario pengujian dengan tujuan penelitian	Skenario pengujian telah sesuai dengan tujuan penelitian dan mampu membuktikan keberhasilan implementasi sistem.
2	Kejelasan prosedur pengujian sistem	Tahapan pengujian sistem dijelaskan dengan cukup jelas dan mudah dipahami.
3	Ketepatan penggunaan metode *Black Box Testing*	Penggunaan metode *Black Box Testing* sudah sesuai untuk menguji fungsi utama sistem jaringan yang dibangun.
4	Kesesuaian hasil pengujian dengan implementasi sistem	Hasil pengujian menunjukkan bahwa sistem berjalan sesuai dengan konfigurasi dan tujuan implementasi.

Lembar Penilaian Validasi Ahli		
No	**Aspek yang dinilai**	**Penliaian Ahli**
5	Kejelasan analisis hasil pengujian	Analisis hasil pengujian telah dijelaskan dengan baik dan memiliki keterkaitan dengan penelitian terdahulu.
Aspek Kelayakan Penelitian		
1	Penelitian relevan dengan kebutuhan jaringan RT/RW-Net	Penelitian memiliki relevansi yang baik terhadap kebutuhan pengelolaan jaringan RT/RW-Net.
2	Penelitian memberikan solusi terhadap masalah jaringan	Implementasi PPPoE mampu memberikan solusi terhadap permasalahan autentikasi dan keamanan jaringan.
3	Implementasi sistem mudah diterapkan	Sistem yang dibangun relatif mudah diterapkan dan dikembangkan pada lingkungan jaringan serupa.
4	Penelitian memiliki manfaat praktis	Penelitian memberikan manfaat praktis bagi pengelolaan jaringan internet berbasis MikroTik.
5	Penelitian layak untuk diterapkan lebih lanjut	Penelitian dinilai layak untuk diterapkan dan dikembangkan lebih lanjut pada jaringan RT/RW-Net.
Saran: Penelitian telah menunjukkan implementasi sistem PPPoE berbasis *MikroTik* yang berjalan dengan baik sesuai tujuan penelitian. Sistem mampu meningkatkan autentikasi pengguna, keamanan akses jaringan, serta pengelolaan *Flat network* pada jaringan RT/RW-Net. Perlu dilakukan pengembangan lebih lanjut pada aspek keamanan lanjutan dan pengujian dengan jumlah pengguna yang lebih besar.		

Hasil penilaian validasi ahli pada Tabel 2 mengonfirmasi bahwa desain dan implementasi sistem PPPoE berbasis MikroTik telah sepenuhnya sesuai dengan tujuan penelitian. Validator menilai bahwa rancangan topologi jaringan, pengalamatan IP, serta penggunaan metode *Network Development Life Cycle* (NDLC) telah diterapkan secara sistematis dan terstruktur. Selain itu, konfigurasi *firewall* beserta fitur isolasi klien dinyatakan terbukti efektif dalam membatasi komunikasi langsung antar pengguna guna memitigasi kerentanan keamanan. Secara keseluruhan, pengaturan fitur autentikasi dan manajemen lalu lintas dinilai sangat relevan dengan kebutuhan pengelolaan infrastruktur RT/RW-Net skala kecil hingga menengah.

Pada aspek pengujian, pakar menegaskan bahwa skenario *Black Box Testing* yang diterapkan sudah sangat tepat dan mampu membuktikan keberhasilan fungsi utama sistem. Penelitian ini diakui berhasil memberikan solusi praktis yang nyata dalam mengatasi permasalahan autentikasi pengguna dan pemerataan *bandwidth* secara dinamis. Meskipun validator memberikan saran untuk mengkaji keamanan lanjutan dan melakukan pengujian pada jumlah pengguna yang lebih masif di masa mendatang, fungsionalitas sistem saat ini sudah dinilai sangat baik. Berdasarkan

evaluasi komprehensif tersebut, pembaruan infrastruktur jaringan berbasis PPPoE ini dinyatakan sangat layak digunakan tanpa revisi.

5. Tahap *Monitoring*

Pada tahap *monitoring*, peneliti memantau kondisi jaringan secara *real-time* dan dinamis, di mana menu PPP *Active* dan Log *MikroTik* secara efektif menampilkan data identitas pengguna aktif, durasi koneksi, hingga riwayat *login*/*logout* untuk keperluan pelacakan dan deteksi dini masalah. Selain itu, pengawasan lalu lintas data pada *Interface Traffic* (Tx/Rx) menunjukkan fluktuasi aktivitas pengguna yang terpantau dengan jelas sehingga administrator dapat menjaga stabilitas performa jaringan. Pemantauan penggunaan batas kecepatan melalui menu *Simple Queue* juga membuktikan bahwa sistem secara langsung membatasi penggunaan data pelanggan sesuai profil yang ditentukan tanpa adanya ketimpangan pembagian *bandwidth*.

6. Tahap *Management*

Pada tahap management, peneliti melakukan pengendalian operasional jaringan secara terpusat melalui pengelolaan akun pengguna, profil layanan, aturan keamanan, serta perutean akses publik. Melalui menu PPP *Secrets* dan PPP *Profile*, administrator terbukti memiliki fleksibilitas dalam menambah, mengubah, maupun menghapus data pelanggan sekaligus menerapkan kebijakan batas kecepatan internet yang langsung aktif secara otomatis. Di samping itu, manajemen *firewall filter* terbukti berhasil mengisolasi lalu lintas antar-klien, sementara konfigurasi NAT dengan aksi *masquerade* divalidasi sukses menjembatani seluruh jaringan lokal agar dapat mengakses internet secara lancar.

KESIMPULAN DAN REKOMENDASI

Implementasi jaringan *Point-to-Point Protocol over Ethernet* (PPPoE) berbasis *MikroTik* menggunakan metode *Network Development Life Cycle* (NDLC) pada RT/RW-Net ADC-Net di Desa Suruhwadang telah berhasil merancang sistem autentikasi terpusat dan isolasi klien. Berdasarkan hasil pengujian fungsional melalui *Black Box Testing* terhadap tiga perangkat klien dengan sembilan skenario uji, sistem ini mencatatkan tingkat keberhasilan mutlak sebesar 100%. Fitur isolasi klien yang diterapkan terbukti sangat efektif dalam memitigasi kerentanan serangan siber lokal, seperti ARP *Spoofing* dan *NetCut*, dengan tingkat pemblokiran komunikasi antar-pengguna berstatus *Request Timed Out* mencapai 100%. Selain itu, otomatisasi fitur *Simple Queue* dinamis secara presisi mampu

mendistribusikan *bandwidth* sesuai dengan tiga profil layanan komersial, yakni paket reguler 5Mbps, *game* 10Mbps, dan *premium* 20Mbps. Secara keseluruhan, tata kelola protokol PPPoE ini terbukti sangat layak diterapkan karena tidak hanya meningkatkan stabilitas jaringan, tetapi juga menghadirkan efisiensi operasional bagi administrator dengan memangkas prosedur aktivasi manual menjadi otomatis.

Berdasarkan keberhasilan implementasi yang telah dicapai, sistem PPPoE berbasis *MikroTik* ini sangat direkomendasikan untuk digunakan sebagai standar utama tata kelola infrastruktur jaringan RT/RW-Net komunal secara terpusat. Sesuai dengan saran dari hasil validasi ahli, pengelola jaringan disarankan untuk melakukan pengembangan lebih lanjut yang difokuskan pada aspek penguatan keamanan sistem tingkat lanjutan. Penelitian lanjutan juga sangat diperlukan untuk mengkaji pengujian kinerja dan stabilitas sistem dengan melibatkan jumlah perangkat pengguna yang jauh lebih masif dari skala pengujian saat ini. Administrator jaringan juga disarankan untuk secara rutin melakukan pemantauan lalu lintas data secara *real-time* menggunakan menu *Interface Traffic* guna memastikan fluktuasi aktivitas pengguna tetap terpantau dengan baik. Terakhir, pendekatan tata kelola jaringan berbasis komunitas ini disarankan untuk dapat direplikasi oleh masyarakat di kawasan perumahan pinggiran lainnya guna menjembatani ketimpangan akses dan infrastruktur digital secara mandiri.

REFERENSI

1. Arbi, Z. F., & Amrullah, A. (2024). Transformasi Sosial dalam Pendidikan Karakter di Era Digital : Peluang dan Tantangan. *Social Studies in Education*, *02*(02), 191–206.
2. Bumbungan, S. (2025). Peran Dan Perkembangan Jaringan Internet Dalam Mendukung Transformasi Digital Global. *Bulletin of Network Engineer and Informatics*, *3*(1), 11–15.
3. Fadilah, M., Wicaksono, M. A., & Handayanna, F. (2025). JUTEKOM Jurnal Teknologi dan Ilmu Komputer. *JUTEKOM Jurnal Teknologi dan Ilmu Komputer*, *1*(4), 136–143.
4. Firmansyah, A., Sucipto, S., Wardani, A. S., & Syafaat, M. (2025). Implementasi Layanan PPPOE dan Hotspot Dalam Satu Interface Pada Warung Priboemi Menggunakan Metode VLAN. *JSITIK: Jurnal Sistem Informasi dan Teknologi Informasi Komputer*, *3*(2), 77–92.

5. Hasany, I. O., & Setiawan, A. (2025). Penerapan Sistem Billing Management Berbasis PPPoE Untuk Manajemen Pelanggan Internet Pada PT Sistem Interkoneksi Data. *Jurnal Pengabdian Masyarakat Bhinnek*, *4*(2), 2395–2405.
6. Husaini, A., & Sari, I. P. (2023). Konfigurasi dan Implementasi RB750Gr3 sebagai RT-RW Net pada Dusun V Suka Damai Desa Sei Meran. *Jurnal Teknik Informatika*, *2*(4), 151–158.
7. Kurniawan, M. (2025). Kesenjangan Akses Pendidikan Digital Antara Wilayah Perkotaan Dan Pedesaan di Indonesia. *Quiz: Journal of Education and Learning*, *1*(2), 44–53.
8. Nursobah, N., Aditya, P., & Supriady, S. (2023). Implementasi Jaringan PPPOE Dan Hotspot Server RT/RW Net Berbasis Mikrotik Dengan Fitur Mikhmon Di Adinet. *Jurnal Informatika*, *13*(1), 31–39.
9. Prasetyo, F. H., Infitharina, E., & Febriyansyah, M. (2025). Penerapan Metode Network Development Life Cycle (NDLC) dalam Pengembangan Jaringan Komputer. *Journal of Informatics and Communications Technology (JICT)*, *7*(1), 080–087.
10. Prayitno, M. H., & Yasir, M. (2025). Peran Metode Network Development Life Cycle (NDLC) pada Implementasi Failover Base Transceiver Station. *INNOVATIVE: Journal Of Social Science Research*, *5*(2), 2146–2158.
11. Samad, A., Hermanto, H., & Adiman, M. F. (2025). *Jurnal Sistem dan Teknologi Informasi Indonesia Konfigurasi MikroTik RouterOS untuk Manajemen Jaringan pada Infrastruktur Jaringan RT / RW Net MikroTik RouterOS Configuration for Network Management in RT / RW Net Network Infrastructure*. *10*(2), 118–125.
12. Sari, L. O., Safrianti, E., & Wahyuningtias, D. (2024). Analisis Keamanan Jaringan Berbasis Point to Point Protocol Over Ethernet (PPPoE) Menggunakan Mikrotik. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, *4*(3), 943–954.
13. Setyawan, A., Khotimah, D. K., & Febri, W. A. (2025). Dampak Kesenjangan Digital Terhadap Pemerataan Akses dan Kualitas Pendidikan di Daerah 3T (Terdepan , Terluar , Tertinggal) Indonesia. *JIMU: Jurnal Ilmiah Multidisipliner*, *03*(04), 1378–1386.
14. Sugari, D., & Hilalludin, H. (2025). Kesetaraan Akses Pendidikan Teknologi Tantangan dan Peluang di Indonesia dan Dunia. *Journal of Multidisciplinary Research2*, *1*(1), 44–56.

15. Tazak'ka, N. A. A., & Sofyan, A. (2025). Analisis Kinerja Jaringan Internet Dalam Mendukung Pelayanan Di Dinas Sosial Kabupaten Brebes. *Sinergi: Jurnal Ilmiah Multidisiplin*, *1*(2), 1523–1540.