

PERANCANGAN *HOTSPOT* MIKROTIK UNTUK KEAMANAN DAN PEMERATAAN AKSES INTERNET STUDI KASUS: SMK NEGERI 3 PRABUMULIH

Anggi Saputra¹, Iwan Setiawan^{2*}, Hermizahadiwidastra³

^{1,2,3}Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Prabumulih, Prabumulih, Indonesia

e-mail: ¹langgysaputra048@gmail.com, ²iwanhen2@gmail.com*,
³hermiza123@gmail.com

ABSTRAK

Perkembangan teknologi informasi mendorong peningkatan kualitas pengelolaan jaringan internet di lingkungan pendidikan. Di SMK Negeri 3 Prabumulih, seluruh pengguna masih menggunakan satu kata sandi *Wi-Fi* sehingga berisiko terhadap akses ilegal, pengelolaan *bandwidth* yang kurang optimal, serta ketidakmerataan akses internet. Penelitian ini bertujuan merancang *Hotspot* MikroTik untuk mendukung keamanan jaringan dan pemerataan akses internet. Metode penelitian yang digunakan adalah *Network Development Life Cycle* (NDLC) dengan tahapan *Analysis*, *Design*, *Simulation Prototype*, dan *Monitoring*. Rancangan meliputi autentikasi pengguna melalui fitur *Hotspot*, manajemen *bandwidth*, penambahan *access point*, pembatasan hak akses administrator berdasarkan *MAC address*, pemblokiran situs tertentu, serta penerapan *client isolation*. Hasil pengujian menunjukkan bahwa autentikasi *Hotspot* berhasil memberikan akses kepada pengguna dengan *username* dan *password* yang sesuai. Pembagian *bandwidth* berjalan sesuai alokasi, dengan hasil pengujian *download* dan *upload* masing-masing sebesar 4,83 Mbps dan 4,81 Mbps pada ruang kantor, serta 2,88 Mbps dan 2,91 Mbps pada ruang TSM dan TKR. Pengujian pembatasan hak akses administrator melalui Winbox menggunakan *MAC address* terdaftar dan tidak terdaftar menunjukkan bahwa akses dapat dibatasi sesuai konfigurasi. Pengujian pemblokiran situs dan *client isolation* juga menunjukkan hasil sesuai dengan konfigurasi yang diterapkan. Rancangan ini dapat menjadi usulan pengembangan jaringan internet di SMK Negeri 3 Prabumulih.

Kata kunci: Mikrotik; *Hotspot*; autentikasi; keamanan jaringan; *bandwidth*.

ABSTRACT

The advancement of information technology encourages improvements in internet network management in educational environments. At SMK Negeri 3 Prabumulih, all users still use a single Wi-Fi password, which poses a risk of unauthorized access, suboptimal bandwidth management, and unequal internet access. This study aims to design a MikroTik Hotspot to support network security and equitable internet access. The research method used is the Network Development Life Cycle (NDLC), consisting of the Analysis, Design, Simulation Prototype, and Monitoring stages. The design includes user authentication through the Hotspot feature, bandwidth management, the addition of access points, restriction of administrator access based on MAC address, website blocking, and the implementation of client isolation. The test results showed that Hotspot authentication successfully provided access to users with the correct username and password. Bandwidth allocation operated according to the configured limits, with

download and upload results of 4.83 Mbps and 4.81 Mbps, respectively, in the office, and 2.88 Mbps and 2.91 Mbps, respectively, in the TSM and TKR rooms. Testing of administrator access restrictions through Winbox using registered and unregistered MAC addresses showed that access could be restricted according to the configuration. Website blocking and client isolation testing also showed results consistent with the applied configuration. The proposed design can serve as a recommendation for the development of the internet network at SMK Negeri 3 Prabumulih.

Keywords: MikroTik; Hotspot; authentication; network security; bandwidth.

1. PENDAHULUAN

Perkembangan teknologi informasi, khususnya internet, mengalami kemajuan yang pesat seiring dengan meningkatnya kebutuhan terhadap akses informasi dan komunikasi. Ketersediaan jaringan internet yang aman, stabil, dan merata menjadi salah satu faktor penting dalam mendukung kegiatan belajar mengajar berbasis digital. Pengelolaan dan perancangan jaringan yang baik diperlukan agar infrastruktur jaringan dapat mendukung kebutuhan pengguna serta menunjang proses kegiatan di lingkungan sekolah [1].

SMK Negeri 3 Prabumulih merupakan salah satu sekolah kejuruan yang telah memanfaatkan jaringan internet untuk mendukung kegiatan akademik dan administrasi. Namun, berdasarkan hasil observasi, pengelolaan jaringan masih menggunakan satu kata sandi *Wi-Fi* yang digunakan secara bersama oleh pengguna sehingga berpotensi menyebabkan kata sandi diketahui oleh pengguna yang tidak berwenang. Selain itu, pengelolaan *bandwidth* belum diterapkan secara optimal sehingga pembagian akses internet belum teratur [2]. Jaringan internet juga masih terbatas pada ruang kantor, sedangkan ruang praktik Teknik Sepeda Motor (TSM) dan Teknik Kendaraan Ringan (TKR) belum memperoleh akses internet yang memadai.

Penelitian mengenai pengelolaan jaringan pada lingkungan pendidikan menunjukkan bahwa penerapan *Hotspot* berbasis MikroTik dapat digunakan untuk mengatur akses pengguna sekaligus mendukung pengelolaan *bandwidth* secara lebih terstruktur [3]. Penelitian lainnya menunjukkan bahwa pengelolaan pengguna dan *bandwidth* pada jaringan sekolah dapat membantu menjaga kestabilan akses internet ketika digunakan oleh banyak pengguna secara bersamaan [4]. Selain itu, penerapan *firewall filtering* pada router MikroTik dapat digunakan sebagai salah satu mekanisme untuk mengendalikan dan membatasi akses terhadap situs atau layanan tertentu dalam jaringan sekolah [5]. Pengoptimalan infrastruktur *Wi-Fi* melalui penempatan *access point* dan pengaturan alokasi *bandwidth* juga dapat membantu meningkatkan kualitas layanan jaringan pada lingkungan pendidikan [6].

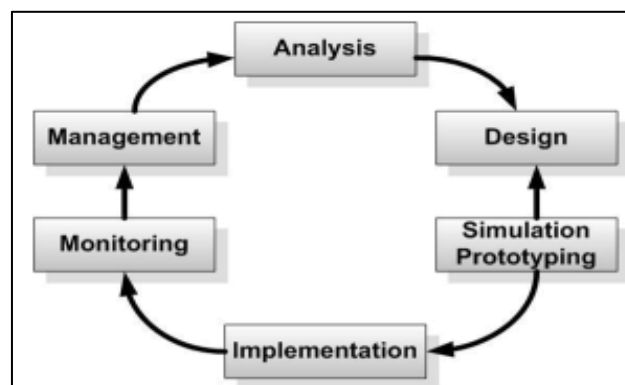
Berdasarkan penelitian terdahulu tersebut, berbagai aspek pengelolaan jaringan seperti autentikasi pengguna, manajemen *bandwidth*, pengendalian akses, *firewall filtering*, dan optimalisasi infrastruktur telah diterapkan secara terpisah maupun pada konteks jaringan pendidikan. Namun, masih diperlukan rancangan yang mengintegrasikan beberapa aspek tersebut sesuai dengan kondisi dan kebutuhan pada lingkungan sekolah. Pada penelitian ini, fitur *Hotspot* MikroTik digunakan untuk menyediakan mekanisme autentikasi pengguna, kemudian dikombinasikan dengan pengelolaan *bandwidth*, penambahan *access point*, pembatasan hak akses administrator, pemblokiran situs tertentu, serta *client isolation* dalam satu rancangan jaringan.

Kontribusi penelitian ini adalah menghasilkan rancangan *Hotspot* MikroTik yang mengintegrasikan pengelolaan akses pengguna, distribusi *bandwidth*, perluasan akses internet, dan beberapa konfigurasi keamanan jaringan sesuai dengan kebutuhan SMK Negeri 3 Prabumulih. Rancangan tersebut diuji melalui beberapa skenario, meliputi pengujian autentikasi pengguna, pembagian *bandwidth*, pembatasan hak akses administrator berdasarkan MAC address, pemblokiran situs tertentu, dan *client isolation*. Pengujian dilakukan untuk mengetahui kesesuaian fungsi setiap konfigurasi dengan rancangan yang telah dibuat.

Berdasarkan uraian tersebut, penelitian ini bertujuan merancang *Hotspot* MikroTik untuk mendukung keamanan dan pemerataan akses internet di SMK Negeri 3 Prabumulih. Metode penelitian yang digunakan adalah *Network Development Life Cycle* (NDLC) dengan tahapan *Analysis*, *Design*, *Simulation Prototype*, dan *Monitoring*. Rancangan yang dihasilkan diharapkan dapat menjadi acuan bagi sekolah dalam mengembangkan jaringan internet yang lebih aman, terstruktur, dan sesuai dengan kebutuhan pengguna.

2. METODE PENELITIAN

Penelitian ini dilakukan pada bulan Desember 2025 sampai dengan Mei 2026 di SMK Negeri 3 Prabumulih. Metode yang dipakai dalam penelitian ini adalah *Network Development Life Cycle* (NDLC) [7]. Metode NDLC mencakup enam tahapan, yaitu *Analysis*, *Design*, *Simulation Prototype*, *Implementation*, *Monitoring*, dan *Management* [8]. Namun, tahapan yang digunakan dalam penelitian ini terdiri atas *Analysis*, *Design*, *Simulation Prototype*, dan *Monitoring*. Adapun tahapan-tahapan tersebut merupakan bagian dari metode *Network Development Life Cycle* (NDLC) yang dapat dilihat pada Gambar 1.



Gambar 1. Metode NDLC

Analysis

Tahap awal ini dilakukan untuk menganalisis kebutuhan jaringan, permasalahan yang ada, serta kondisi jaringan saat ini [9]. Analisis dilakukan melalui observasi langsung pada ruang kantor, ruang praktik Teknik Sepeda Motor (TSM), dan ruang praktik Teknik Kendaraan Ringan (TKR). Selain itu, dilakukan pengumpulan informasi mengenai perangkat jaringan yang digunakan, kondisi infrastruktur, serta kebutuhan pengembangan jaringan sebagai dasar dalam penyusunan rancangan jaringan

Design

Pada tahap ini dibuat rancangan jaringan berdasarkan hasil analisis kebutuhan [10]. Tahap *design* dilakukan untuk membuat gambar topologi jaringan yang akan dibangun sesuai dengan hasil analisis [11]. Perancangan meliputi penyusunan rancangan koneksi jaringan antara ruang kantor dengan ruang praktik TSM dan TKR, penempatan *access point*, serta konfigurasi *router* mikrotik sebagai pusat pengelolaan jaringan. Selain itu, dirancang penerapan autentikasi pengguna melalui fitur *Hotspot*, manajemen *bandwidth*, pembatasan hak akses administrator berdasarkan *MAC address*, pemblokiran situs tertentu, dan *client isolation* untuk melindungi perangkat dari gangguan antar pengguna dalam jaringan.

Simulation Prototype

Tahap *simulation prototype* merupakan tahap pembangunan prototipe jaringan berdasarkan rancangan yang telah dibuat [12]. Pada tahap ini dilakukan konfigurasi jaringan menggunakan perangkat berupa modem, *router* MikroTik, *switch*, dan *access point*. Simulasi dilakukan dengan menghubungkan seluruh perangkat jaringan sesuai dengan topologi yang telah dirancang. Selanjutnya dilakukan konfigurasi pada *router* MikroTik yang meliputi autentikasi pengguna melalui fitur *Hotspot*, manajemen *bandwidth*, pembatasan hak akses administrator berdasarkan *MAC address*, pemblokiran situs tertentu, serta penerapan *client isolation* untuk melindungi perangkat dari gangguan antar pengguna dalam jaringan. Simulasi ini dilakukan untuk memastikan seluruh konfigurasi dapat berjalan sesuai dengan rancangan sebelum dilakukan tahap monitoring.

Monitoring

Tahapan monitoring merupakan tahapan yang penting agar jaringan dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari *user* pada tahap analisis [13]. Tahap monitoring dilakukan untuk memantau jalannya simulasi dan implementasi terbatas yang telah dilakukan. Pemantauan meliputi pengujian autentikasi pengguna melalui *Hotspot*, pembagian *bandwidth*, pembatasan hak akses administrator pada *router* MikroTik berdasarkan *MAC address*, pengujian pemblokiran terhadap situs tertentu, serta pengujian *client isolation* untuk melindungi perangkat dari gangguan antar pengguna dalam jaringan [14]. Tahap ini bertujuan untuk mengevaluasi kesesuaian antara rancangan jaringan dengan proses yang dijalankan selama penelitian [15].

3. HASIL DAN PEMBAHASAN

Hasil

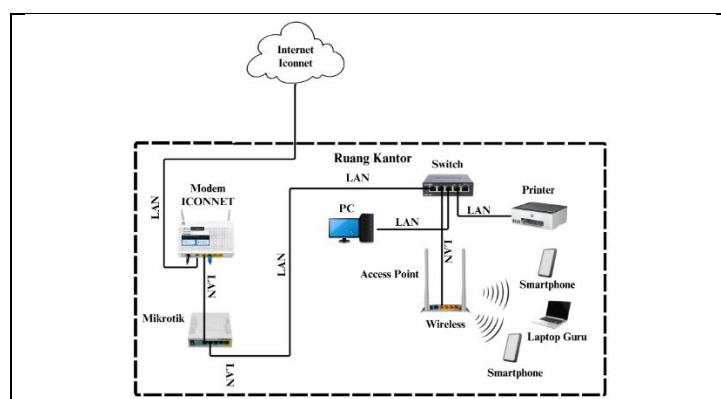
Pada bagian ini disajikan hasil penelitian berdasarkan tahapan metode *Network Development Life Cycle* (NDLC) yang meliputi *Analysis*, *Design*, *Simulation Prototype*, dan *Monitoring*. Setiap tahapan menjelaskan proses perancangan, simulasi, implementasi terbatas, serta evaluasi jaringan yang dilakukan di SMK Negeri 3 Prabumulih. Hasil yang diperoleh menunjukkan proses pengembangan jaringan mulai dari identifikasi permasalahan, perancangan solusi, pengujian konfigurasi, hingga pemantauan terhadap penerapan autentikasi pengguna melalui fitur *Hotspot*, manajemen *bandwidth*, pembatasan hak akses administrator berdasarkan *MAC address*, pemblokiran situs tertentu, dan *client isolation*.

Analysis

Pada tahap *analysis* dilakukan identifikasi kondisi jaringan internet di SMK Negeri 3 Prabumulih melalui observasi langsung. Berdasarkan hasil observasi, terdapat 17 guru, 17 siswa Program Keahlian Teknik Sepeda Motor (TSM), dan 32 siswa Program Keahlian Teknik Kendaraan Ringan (TKR). Sumber internet berasal dari layanan *ICONNET* yang terhubung ke modem di ruang kantor dan didistribusikan melalui kabel LAN.

Jaringan internet yang tersedia masih terpusat di ruang kantor, sedangkan ruang praktik TSM dan TKR belum memiliki *access point*. Selain itu, akses *Wi-Fi* masih menggunakan satu kata sandi secara bersama sehingga autentikasi pengguna belum dilakukan secara individual. Pengelolaan *bandwidth* juga belum diterapkan secara terstruktur dan beberapa konfigurasi keamanan jaringan belum tersedia.

Berdasarkan kondisi tersebut, diperlukan rancangan *Hotspot* MikroTik yang mencakup autentikasi pengguna, pengelolaan *bandwidth*, penambahan *access point* pada ruang praktik TSM dan TKR, serta konfigurasi keamanan berupa pembatasan akses administrator berdasarkan *MAC address*, pemblokiran situs tertentu, dan *client isolation*. Rancangan tersebut selanjutnya diuji melalui simulasi untuk mengetahui kesesuaian setiap konfigurasi dengan kebutuhan jaringan sekolah.



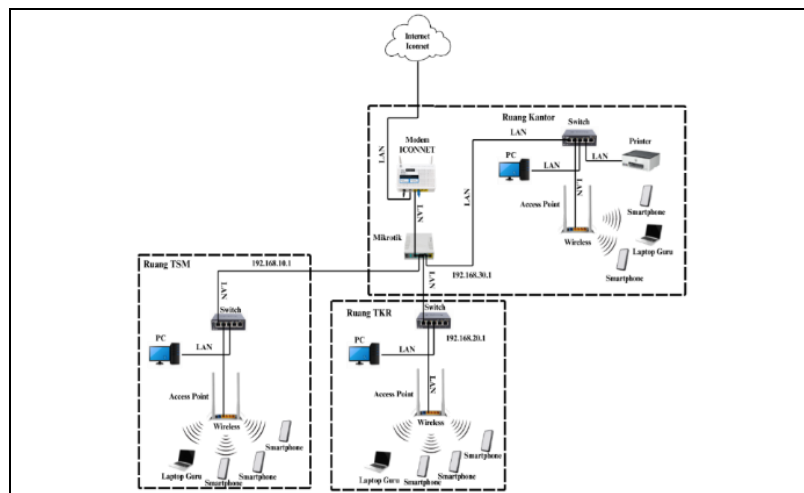
Gambar 2. Jaringan Lama

Berdasarkan hasil identifikasi tersebut, dapat disimpulkan beberapa permasalahan jaringan di SMK Negeri 3 Prabumulih, yaitu:

1. Jaringan internet hanya tersedia di ruang kantor, sedangkan ruang praktik TSM dan TKR belum memperoleh akses internet.
2. Akses *Wi-Fi* masih menggunakan satu kata sandi yang digunakan secara bersama oleh pengguna sehingga autentikasi pengguna belum dilakukan secara individual.
3. Pengelolaan *bandwidth* belum diterapkan secara terstruktur sehingga pembagian akses internet belum dapat dikendalikan secara optimal.
4. Belum diterapkan pembatasan hak akses administrator berdasarkan *MAC address*, pemblokiran situs tertentu, serta mekanisme *client isolation* untuk membatasi komunikasi antarperangkat dalam jaringan.

Design

Pada tahap ini peneliti merancang topologi jaringan sesuai dengan kondisi dan kebutuhan jaringan di SMK Negeri 3 Prabumulih. Perancangan dilakukan dengan memanfaatkan jaringan internet yang telah tersedia di ruang kantor, kemudian memperluas jangkauan jaringan ke ruang praktik Teknik Sepeda Motor (TSM) dan Teknik Kendaraan Ringan (TKR). Selain itu, dirancang penerapan *Hotspot* MikroTik untuk autentikasi pengguna, manajemen *bandwidth*, serta konfigurasi keamanan jaringan. Gambar 3 merupakan rancangan topologi jaringan yang direkomendasikan untuk diterapkan di SMK Negeri 3 Prabumulih.



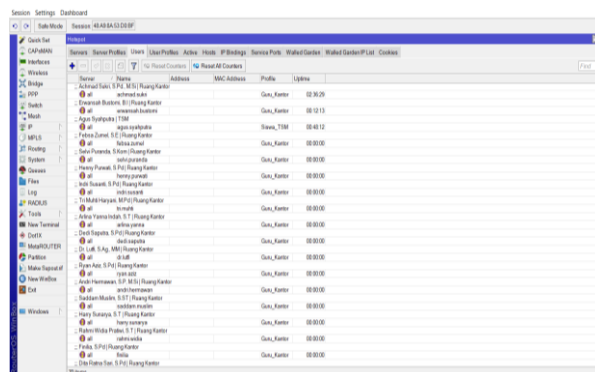
Gambar 3. Topologi Jaringan yang direkomendasikan

Berikut penjelasan mengenai rancangan jaringan pada Gambar 3 yang terdiri atas beberapa perangkat yang saling terhubung untuk mendukung autentikasi pengguna, pengelolaan *bandwidth*, perluasan akses, dan keamanan jaringan:

1. Sumber internet berasal dari layanan *ICONNET* yang terhubung ke modem *ICONNET* sebagai penerima koneksi internet dari penyedia layanan.
2. Modem *ICONNET* dihubungkan ke *router* MikroTik melalui kabel LAN. *Router* MikroTik berfungsi sebagai pusat pengelolaan jaringan, termasuk autentikasi pengguna melalui fitur *Hotspot*, pengaturan *bandwidth*, dan konfigurasi keamanan jaringan.
3. *Router* MikroTik dihubungkan ke *switch* di ruang kantor sebagai media distribusi jaringan ke perangkat seperti PC, *access point*, printer, dan perangkat pengguna.
4. *Router* MikroTik juga dihubungkan ke *switch* pada ruang praktik TSM melalui kabel LAN untuk mendistribusikan koneksi jaringan ke ruangan tersebut.
5. *Switch* pada ruang praktik TSM dihubungkan ke *access point* sehingga perangkat seperti laptop dan *smartphone* dapat mengakses internet melalui autentikasi *Hotspot*.
6. *Router* MikroTik selanjutnya dihubungkan ke *switch* pada ruang praktik TKR melalui kabel LAN untuk mendistribusikan koneksi jaringan ke ruangan tersebut.
7. *Switch* pada ruang praktik TKR dihubungkan ke *access point* sehingga perangkat seperti laptop dan *smartphone* dapat mengakses internet melalui autentikasi *Hotspot*.

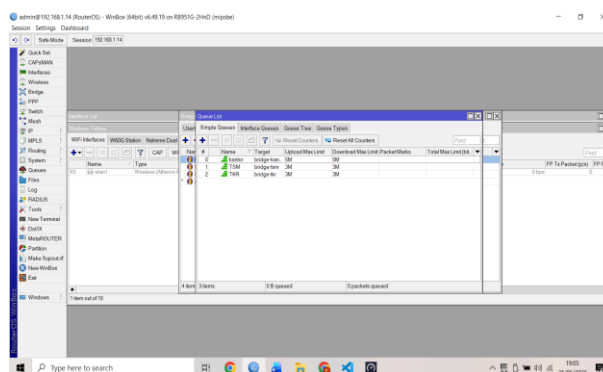
Simulation Prototype

Pada tahap ini dilakukan simulasi jaringan berdasarkan topologi yang telah dirancang menggunakan *modem*, *router* Mikrotik, *switch*, dan *access point*. Konfigurasi meliputi autentikasi *Hotspot*, manajemen *bandwidth*, pembatasan hak akses administrator, pemblokiran situs, serta penerapan *client isolation* untuk meningkatkan keamanan jaringan.



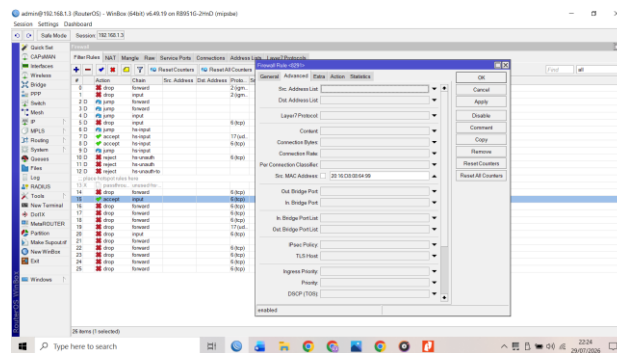
Gambar 4. *Username dan Password User*

Gambar 4 menunjukkan konfigurasi autentikasi *Hotspot* pada *router* Mikrotik dengan membuat *username* dan *password* bagi pengguna. Setiap pengguna diwajibkan melakukan *login* sebelum memperoleh akses internet.



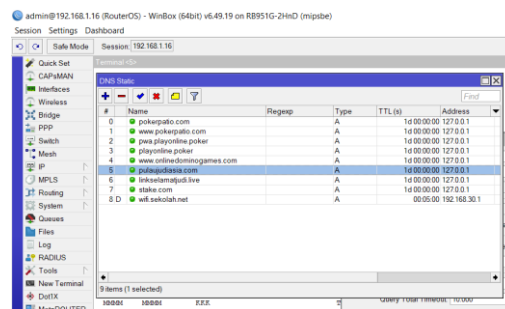
Gambar 5. *Manajemen Bandwidth User*

Gambar 5 menunjukkan konfigurasi *Simple Queue* untuk mengatur pembagian *bandwidth* berdasarkan kebutuhan pengguna sehingga akses internet dapat digunakan secara lebih merata.



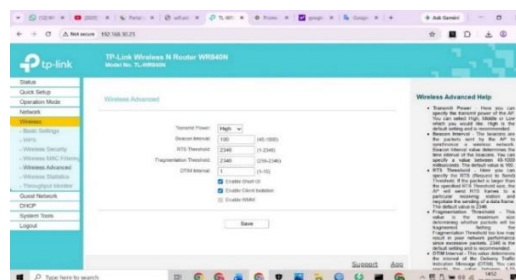
Gambar 6. Konfigurasi Hak Akses Administrator

Gambar 6 menunjukkan pembatasan hak akses administrator pada *router* Mikrotik agar pengelolaan konfigurasi jaringan hanya dapat dilakukan oleh pengguna yang memiliki hak akses.



Gambar 7. Konfigurasi Blok Situs

Gambar 7 menunjukkan konfigurasi pemblokiran situs pada *router* Mikrotik untuk membatasi akses ke situs yang tidak sesuai dengan lingkungan pendidikan.



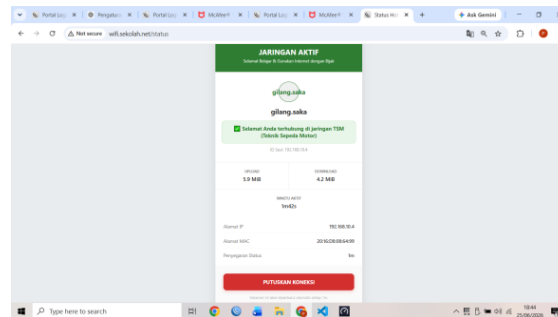
Gambar 8. Konfigurasi Mekanisme Keamanan Untuk Antar User

Gambar 8 menunjukkan penerapan fitur *client isolation* pada *access point* untuk membatasi komunikasi langsung antarperangkat pengguna sehingga keamanan jaringan dapat ditingkatkan.

Monitoring

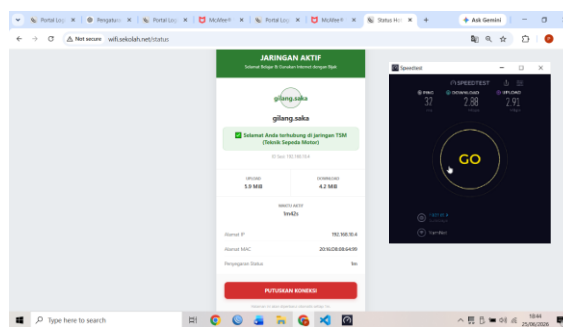
Pada tahap ini dilakukan monitoring terhadap konfigurasi jaringan pada *router* MikroTik dan *access point* untuk memeriksa penerapan setiap konfigurasi yang telah dirancang. Monitoring meliputi autentikasi *Hotspot*, manajemen *bandwidth*, pembatasan hak akses administrator, pemblokiran situs, dan penerapan *client isolation*. Monitoring

dilakukan pada setiap konfigurasi yang telah diterapkan sesuai dengan rancangan jaringan.



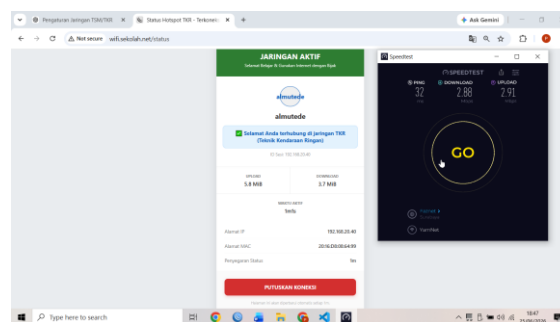
Gambar 9. Halaman *Login Hotspot* MikroTik

Pengujian dilakukan melalui halaman *login Hotspot* MikroTik dengan memasukkan *username* dan *password* yang telah dikonfigurasi. Proses ini dilakukan untuk menguji mekanisme autentikasi pengguna pada jaringan *Hotspot*.



Gambar 10. Menggunakan Aplikasi *Speedtest* di Ruang TSM

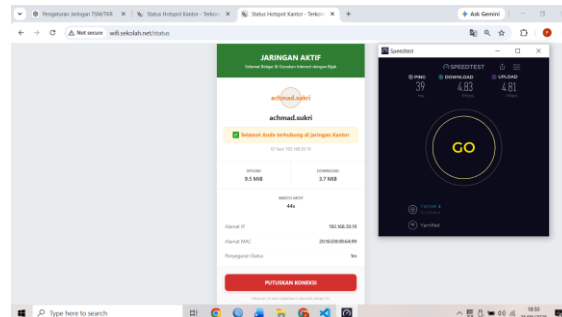
Pengujian pada ruang TSM dilakukan dengan mengakses jaringan *Hotspot* yang telah dikonfigurasi pada MikroTik. Setelah pengguna berhasil melakukan autentikasi, dilakukan pengukuran kecepatan internet menggunakan *Speedtest* untuk mengetahui hasil *download* dan *upload* yang diperoleh pada ruang TSM.



Gambar 11. Menggunakan Aplikasi *Speedtest* di Ruang TKR

Pada ruang TKR, pengujian dilakukan dengan menghubungkan perangkat pengguna ke jaringan *Hotspot* sesuai konfigurasi yang telah ditentukan. Selanjutnya,

Speedtest digunakan untuk mengukur performa koneksi internet yang diterima pengguna pada ruang TKR, meliputi kecepatan *download* dan *upload*.



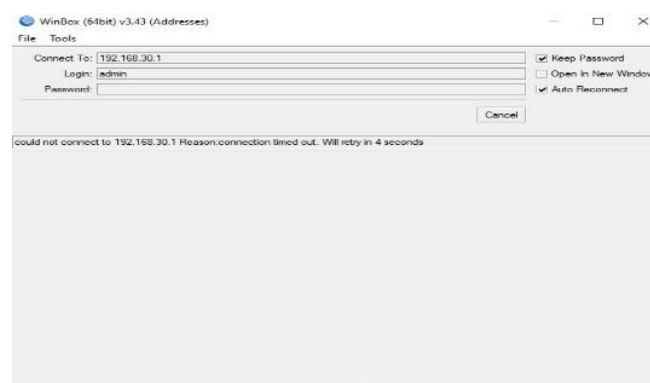
Gambar 12. Menggunakan Aplikasi *Speedtest* di Ruang Kantor

Pengujian di ruang kantor dilakukan setelah perangkat terhubung melalui jaringan *Hotspot*. Pengukuran menggunakan *Speedtest* dilakukan untuk melihat kemampuan koneksi internet pada area kantor berdasarkan pembagian *bandwidth* yang telah diterapkan pada MikroTik.



Gambar 13. MAC yang Sesuai dengan Laptop Admin

Proses akses administrator dilakukan menggunakan laptop dengan *MAC address* yang telah terdaftar pada konfigurasi MikroTik. Pengujian dilakukan melalui aplikasi WinBox untuk memastikan perangkat administrator dapat mengakses *router*.



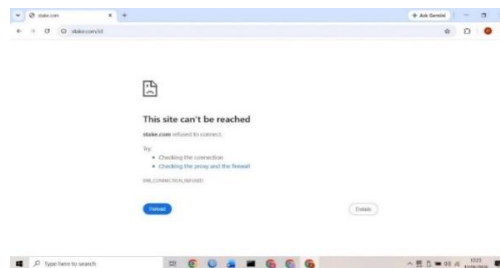
Gambar 14. MAC Laptop yang Berbeda

Proses akses administrator dilakukan menggunakan laptop dengan *MAC address* yang berbeda dari *MAC address* yang telah terdaftar pada konfigurasi MikroTik. Pengujian dilakukan melalui aplikasi Winbox untuk menguji akses perangkat ke *router*.



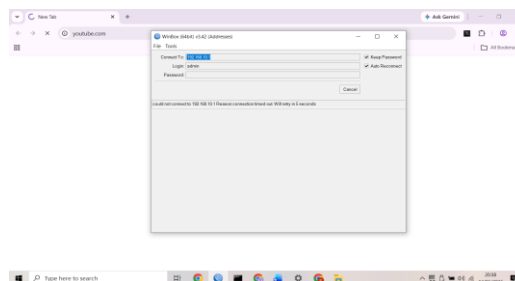
Gambar 15. Salah Satu *Website* Judi Sebelum di *Block*

Pengujian dilakukan dengan mengakses situs yang menjadi objek pemblokiran melalui jaringan *Hotspot* sebelum aturan pemblokiran diterapkan pada MikroTik. Pengujian ini digunakan sebagai kondisi awal sebelum konfigurasi pemblokiran dilakukan.



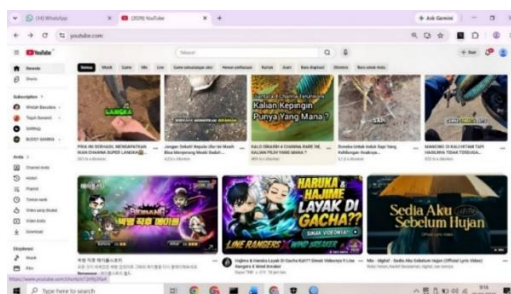
Gambar 16. Sesudah di *Block*

Pengujian dilakukan kembali pada situs yang sama setelah aturan pemblokiran dikonfigurasi pada MikroTik. Pengujian ini digunakan untuk melihat kondisi akses situs setelah penerapan konfigurasi pemblokiran



Gambar 17. Sebelum Diterapkan *Client Isolation*

Pengujian dilakukan dengan menghubungkan beberapa perangkat pada *access point* yang sama. Aplikasi NetCut digunakan untuk melakukan pengujian terhadap koneksi antarperangkat yang terhubung pada jaringan.



Gambar 18. Sesudah Diterapkan *Client Isolation*

Pengujian dilakukan kembali menggunakan beberapa perangkat yang terhubung pada *access point*. Aplikasi NetCut digunakan untuk menguji koneksi antarperangkat setelah konfigurasi *client isolation* diterapkan pada jaringan.

Pembahasan

Pada tahap pembahasan, hasil pengujian terhadap rancangan jaringan dianalisis berdasarkan aspek autentikasi pengguna, pengelolaan *bandwidth*, pembatasan hak akses administrator, pemblokiran situs, dan penerapan *client isolation*. Analisis dilakukan untuk mengetahui kesesuaian antara konfigurasi yang diterapkan dengan hasil pengujian pada masing-masing aspek. Hasil pengujian dan analisis setiap aspek disajikan pada Tabel 1 sampai Tabel 5.

Tabel 1. Hasil Pengujian Autentikasi

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil Pengujian	Status
1	<i>Login dengan Username Password Benar</i>	Berhasil Masuk ke Jaringan <i>Hotspot</i>	Berhasil masuk ke jaringan dan memperoleh akses internet	Berhasil

Berdasarkan Tabel 1, hasil pengujian autentikasi menunjukkan bahwa pengguna yang memasukkan *username* dan *password* yang telah dikonfigurasi dapat melakukan login pada jaringan *Hotspot*. Setelah proses autentikasi dilakukan, pengguna memperoleh akses internet sesuai dengan konfigurasi jaringan yang diterapkan. Hasil tersebut menunjukkan bahwa mekanisme autentikasi *Hotspot* pada MikroTik dapat digunakan untuk mengatur akses pengguna sebelum memperoleh koneksi internet. Penerapan *username* dan *password* secara individual juga memberikan mekanisme pengelolaan akses yang berbeda dibandingkan penggunaan satu kata sandi *Wi-Fi* secara bersama-sama.

Tabel 2. Hasil Pengujian *Bandwidth*

No	Pengujian Jaringan	Batas <i>Bandwidth</i>	Hasil <i>Download</i> (Mbps)	Hasil <i>Upload</i> (Mbps)	Status
1	Ruang Kantor	5 Mbps	4,83	4,81	Berhasil
2	Ruang TSM	3 Mbps	2,88	2,91	Berhasil

3	Ruang TKR	3 Mbps	2,88	2,91	Berhasil
---	-----------	--------	------	------	----------

Berdasarkan Tabel 2, hasil pengujian menunjukkan bahwa pembagian *bandwidth* dapat diterapkan pada masing-masing ruang sesuai dengan batas yang telah ditentukan. Ruang Kantor memiliki batas *bandwidth* sebesar 5 Mbps dengan hasil pengukuran *download* sebesar 4,83 Mbps dan *upload* sebesar 4,81 Mbps. Ruang TSM dan TKR masing-masing memiliki batas *bandwidth* sebesar 3 Mbps dengan hasil *download* sebesar 2,88 Mbps dan *upload* sebesar 2,91 Mbps. Nilai hasil pengukuran yang mendekati batas konfigurasi menunjukkan bahwa pembagian *bandwidth* dapat diterapkan sesuai dengan alokasi yang telah dirancang. Perbedaan alokasi antara ruang kantor dan ruang TSM serta TKR menunjukkan adanya pengaturan penggunaan *bandwidth* berdasarkan kebutuhan masing-masing area jaringan.

Tabel 3. Hasil Pengujian Hak Administrator

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil Pengujian	Status
1	MAC Address administrator terdaftar	Berhasil Login ke Winbox	Berhasil Login ke Winbox	Berhasil
2	MAC Address administrator tidak terdaftar	Tidak Dapat Login ke Winbox	Login Ditolak	Berhasil

Berdasarkan Tabel 3, hasil pengujian menunjukkan adanya perbedaan akses antara perangkat dengan MAC address yang telah terdaftar dan perangkat dengan MAC address yang tidak terdaftar. Perangkat administrator yang memiliki MAC address terdaftar dapat melakukan *login* ke MikroTik melalui Winbox, sedangkan perangkat dengan MAC address yang tidak terdaftar memperoleh penolakan akses dengan kondisi *connection timed out*. Hasil tersebut menunjukkan bahwa pembatasan berdasarkan MAC address dapat diterapkan untuk mengatur perangkat yang diperbolehkan mengakses konfigurasi *router*. Konfigurasi ini membatasi pengelolaan *router* hanya pada perangkat administrator yang telah ditentukan dalam rancangan jaringan.

Tabel 4. Hasil Pengujian Pemblokiran Situs

No	Kondisi Pengujian	Hasil yang Diharapkan	Hasil Pengujian	Status
1	Sebelum Pemblokiran	Situs <i>stake.com</i> dapat di akses	Berhasil Diakses	Berhasil
2	Sesudah Pemblokiran	Situs <i>stake.com</i> tidak dapat di akses	Akses ke <i>stake.com</i> diblokir	Berhasil

Berdasarkan Tabel 4, hasil pengujian dilakukan dengan membandingkan akses terhadap situs *stake.com* sebelum dan sesudah aturan pemblokiran diterapkan pada MikroTik. Sebelum konfigurasi pemblokiran diterapkan, situs tersebut masih dapat diakses melalui jaringan *Hotspot*. Setelah aturan pemblokiran diterapkan, akses menuju

stake.com diblokir dan *browser* menampilkan pesan “*This site can't be reached*”. Hasil tersebut menunjukkan bahwa aturan pemblokiran pada MikroTik dapat diterapkan untuk membatasi akses terhadap situs yang telah ditentukan. Penerapan konfigurasi ini menjadi salah satu bentuk pengendalian akses internet yang dapat disesuaikan dengan kebutuhan penggunaan jaringan di lingkungan sekolah.

Tabel 5. Hasil Pengujian Mekanisme Keamanan Antar Pengguna

No	Kondisi Pengujian	Hasil yang Diharapkan	Hasil Pengujian	Status
1	Sebelum Penerapan <i>Client Isolation</i>	Koneksi dapat diganggu	Koneksi terputus	Berhasil
2	Sesudah penerapan <i>Client Isolation</i>	Koneksi tetap aman	Internet tetap terhubung	Berhasil

Berdasarkan Tabel 5, hasil pengujian menunjukkan adanya perbedaan kondisi koneksi sebelum dan sesudah penerapan *client isolation*. Sebelum fitur diterapkan, pengujian menggunakan NetCut menunjukkan bahwa koneksi perangkat target dapat terganggu hingga menyebabkan koneksi internet terputus. Setelah *client isolation* diterapkan pada *access point*, perangkat target tetap terhubung ke internet meskipun dilakukan percobaan gangguan menggunakan NetCut. Hasil tersebut menunjukkan bahwa *client isolation* dapat membatasi komunikasi langsung antarperangkat yang terhubung pada *access point* yang sama. Penerapan mekanisme ini mendukung aspek keamanan antar pengguna dengan mengurangi potensi gangguan terhadap koneksi perangkat lain dalam jaringan.

4. KESIMPULAN

Berdasarkan hasil penelitian, telah dirancang dan disimulasikan jaringan *Hotspot* MikroTik di SMK Negeri 3 Prabumulih untuk meningkatkan keamanan dan pemerataan akses internet melalui autentikasi pengguna, manajemen *bandwidth*, pembatasan hak akses administrator, pemblokiran situs, dan *client isolation*. Pengujian autentikasi dilakukan dengan *login* menggunakan *username* dan *password* yang telah dikonfigurasi, sedangkan pengujian *bandwidth* dilakukan menggunakan *Speedtest* pada ruang kantor, TSM, dan TKR. Hasil pengukuran menunjukkan kecepatan *download* dan *upload* masing-masing sebesar 4,83 Mbps dan 4,81 Mbps pada ruang kantor, serta 2,88 Mbps dan 2,91 Mbps pada ruang TSM dan TKR dengan alokasi *bandwidth* masing-masing 5 Mbps untuk kantor dan 3 Mbps untuk TSM serta TKR. Pengujian hak akses administrator dilakukan melalui Winbox menggunakan perangkat dengan MAC *address* terdaftar dan tidak terdaftar, pengujian pemblokiran dilakukan dengan mengakses situs *stake.com* sebelum dan sesudah konfigurasi pemblokiran, sedangkan pengujian *client isolation* dilakukan menggunakan NetCut untuk menguji koneksi antarperangkat. Hasil pengujian menunjukkan bahwa konfigurasi yang diterapkan dapat berjalan sesuai rancangan. Penelitian ini memiliki keterbatasan pada jumlah perangkat yang digunakan dalam

pengujian, sehingga penerapan dengan jumlah pengguna dan perangkat yang lebih besar diperlukan untuk mengetahui kinerja jaringan pada kondisi penggunaan yang lebih luas.

DAFTAR PUSTAKA

- [1] L. Sondey, R. Harijadi Wibowo Pardanus, And P. Veronica Togas, “Analisis Dan Perancangan Jaringan Komputer Di SMK,” *Jurnal Pendidikan Teknologi Informasi Dan Komunikasi*, Vol. 2, No. 5, Oct. 2022.
- [2] A. Fauzi, M. Ficky Duskarnaen, And H. Ajie, “Desain Dan Implementasi Management Bandwidth Pada *Hotspot* Mikrotik Di Smk Mutiara 17 Agustus Bekasi,” *Jurnal Pinter*, Vol. 6, No. 1, Pp. 73–78, Jun. 2022, doi: <https://doi.org/10.21009/Pinter.6.1.10>.
- [3] D. Anamatalu, F. Hariadi, and R. Mikaela Indri Malo, “Manajemen *User* Dan *Bandwidth* Pada Jaringan *Hotspot* Menggunakan Mikrotik di Sekolah Menengah Kejuruan Negeri 5 Waingapu,” *SABER Jurnal Teknik Informatika, Sains Dan Ilmu Komunikasi*, Vol. 2, No. 1, Pp. 254–269, Jan. 2024, doi: [10.59841/Saber.V2i1.603](https://doi.org/10.59841/Saber.V2i1.603).
- [4] N. Asyifah and D. Ramayanti, “Optimasi Kinerja Jaringan Di Smk Al Fudhola Bekasi: Pengaturan *Bandwidth* Dengan Mikrotik Rb 951ui-2hnd Dan Penerapan Algoritma *Simple Queue*,” *Jurnal Ilmiah Ilkominfo*, Vol. 7, Pp. 2621–4962, Jan. 2024.
- [5] K. Aziz, S. Zakir, W. Aprison, And L. Efriyanti, “Implementasi Keamanan Jaringan Dengan Metode *Firewall Filtering* Menggunakan Mikrotik Di SMKN 3 Payakumbu,” *JATI (Jurnal Mahasiswa Teknik Informatika)*, Vol. 8, No. 3, Jun. 2024.
- [6] D. Ramayanti and V. Saputra, “Optimasi Infrastruktur Wi-Fi Dan Manajemen *Bandwidth* Di Sekolah Menengah Pertama Menggunakan Teknologi Mikrotik,” *Arcitech: Journal of Computer Science and Artificial Intelligence*, Vol. 5, No. 1, Pp. 1–17, Jun. 2025, Doi: [10.29240/Arcitech.V5i1.12408](https://doi.org/10.29240/Arcitech.V5i1.12408).
- [7] L. A. J. Sigit, A. S. Y. Irawan, And D. Juardi, “Analisis Perancangan Arsitektur Jaringan Smk Negeri 3 Kota Bekasi Menggunakan Metode Ndlc Dengan Pemanfaatan *Software-Defined Networking*,” *INFOTECH Journal*, Vol. 9, No. 2, Pp. 520–531, Aug. 2023, Doi: [10.31949/Infotech.V9i2.6536](https://doi.org/10.31949/Infotech.V9i2.6536).
- [8] S. Mitro S, D. Sukma, And H. Permana, “Rancangan Jaringan Komputer Di SMK: Studi Implementasi Menggunakan *Cisco Packet Tracer*,” *JITES*, Vol. 3, No. 2, Pp. 46–51, 2024, [Online]. Available: <https://jites.untara.ac.id/index.php/jites>
- [9] P. Agustina Saho, A. Mewengkang, And A. Cerullo Djamen, “Analisis Dan Perancangan Jaringan Di SMA Negeri 1 Essang,” *Edutik: Jurnal Pendidikan Teknologi Informasi Dan Komunikasi*, Vol. 4, No. 2, Apr. 2024, doi: <https://doi.org/10.53682/Edutik.V3i5.8898>.
- [10] R. Setiawan, M. Ficky Duskarnaen, And H. Ajie, “Perancangan Jaringan Vlan (*Virtual Local Area Network*) Di Smkn 40 Jakarta Dengan Menggunakan Metode NDLC (*Network Development Life Cycle*),” *Pinter: Jurnal Pendidikan Teknik Informatika Dan Komputer*, Vol. 8, No. 1, Pp. 46–53, Jun. 2024, Doi: [10.21009/Pinter.8.1.5](https://doi.org/10.21009/Pinter.8.1.5).

- [11] Subandri, M. Lutfi Sulthon Auliya Sulistyono, D. Suryadi, P. Indah Lestari, A. Ilham Ramdhani, And D. Ginola, “Monitoring Jaringan Menggunakan Aplikasi *The Dude* Dengan Memberikan Notifikasi Melalui Telegram Dan Email (Studi Kasus: Labkom Ftid Universitas Bani Saleh),” *Jurnal Tridi Teknologi Informatika & Komputer*, Vol. 1, Pp. 6–18, Dec. 2023, Accessed: Aug. 02, 2026. [Online]. Available: <https://Banisalehjurnal.Ubs.Ac.Id/Index.Php/Tridi/Article/Download/12/9/32>
- [12] A. Ekklesia Tangkowitz, V. Ronny Palilingan, And O. Eunike Selvie Liando, “Analisis Dan Perancangan Jaringan Komputer Di Sekolah Menengah Pertama,” *Eduatik: Jurnal Pendidikan Teknologi Informasi Dan Komunikasi*, Vol. 1, No. 1, Feb. 2021, Accessed: Aug. 02, 2026. [Online]. Available: <https://Ejurnal.Unima.Ac.Id/Index.Php/Eduatik/Article/Download/1044/1286>
- [13] A. Izzaturrahmah, M. Tahir, N. Hariri, And H. U. A. Putra, “Implementasi Dan Evaluasi Monitoring Pada Jaringan Lokal Berbasis Mikrotik Menggunakan Visualisasi *Graphing* Dan *Graph*,” *Digital Transformation Technology*, Vol. 5, No. 1, Pp. 143–149, May 2025, doi: 10.47709/digitech.v5i1.5883.
- [14] A. K. Septuvania and G. Purnama, “Analisis Dan Perancangan Jaringan Infrastruktur Sekolah MTS Al-Ihsan,” *Jurnal Informatika Dan Teknik Elektro Terapan*, Vol. 11, No. 3, Aug. 2023, Doi: 10.23960/Jitet.V11i3.3314.
- [15] M. Irsyadul Ibad, W. Mahmud, And G. Wilujeng, “Analisis Efektivitas *Firewall* Mikrotik Dalam Mitigasi Serangan Ddos Menggunakan Pendekatan *Network Development Life Cycle* (NDLC),” *Sistemasi: Jurnal Sistem Informasi*, Vol. 15, No. 5, Pp. 1731–1748, May 2026.