

## **Implementasi Infrastruktur Jaringan Internet Berbasis Mikrotik di Marqiz Imam Syafi'i & Musholla Imam Syafii Condet Dengan Sistem Monitoring Jarak Jauh**

**Naufal Azka Syamil\*, Oky Tria Saputra**

Politeknik IDN Bogor, Indonesia

Email: naufalne2109@gmail.com\*

---

**Keywords:**

*computer network; Mikrotik;  
LAN/WLAN; Quality of Service  
(QoS); network monitoring;  
bandwidth management.*

---

**Abstract**

*This research and implementation aim to design and build a more stable, evenly distributed, and controlled internet network infrastructure at Marqiz Imam Syafi'i and Musholla Imam Syafii Condet, East Jakarta. Initial problems included unstable LTE-based connections, limited WiFi coverage, no LAN network for operational devices and CCTV, and no remote monitoring system. The methods used include topology design, Mikrotik router configuration (DHCP, NAT, Hotspot, Queue, Firewall, DDNS), and network performance testing. The results show that after implementation, the connection became more stable, internet coverage is more evenly distributed, and network management and monitoring can be done remotely using DDNS service. Quality of Service (QoS) implementation limits bandwidth to 3 Mbps per hotspot user and 50 Mbps for the Marqiz subnet. The firewall successfully blocks access to online games (Mobile Legends, Free Fire, PUBG, Clash of Clans) and restricts internet access during prayer times. The built infrastructure is also able to support operational activities and live streaming more optimally.*

---

**Kata Kunci:**

jaringan computer; Mikrotik;  
LAN/WLAN; Quality of Service  
(QoS); monitoring jaringan;  
manajemen bandwidth.

---

**Abstrak**

Penelitian dan implementasi ini bertujuan merancang dan membangun infrastruktur jaringan internet yang lebih stabil, merata, dan terkontrol di Marqiz Imam Syafi'i dan Musholla Imam Syafii Condet, Jakarta Timur. Permasalahan awal meliputi koneksi berbasis LTE yang tidak stabil, cakupan WiFi terbatas, belum tersedianya jaringan LAN untuk perangkat operasional dan CCTV, serta tidak adanya sistem monitoring jarak jauh. Metode yang digunakan meliputi perancangan topologi, konfigurasi router Mikrotik (DHCP, NAT, Hotspot, Queue, Firewall, DDNS), dan pengujian kinerja jaringan. Hasil penelitian menunjukkan bahwa setelah implementasi, koneksi menjadi lebih stabil, cakupan internet lebih merata, dan pengelolaan serta pemantauan jaringan dapat dilakukan secara remote menggunakan layanan DDNS. Penerapan Quality of Service (QoS) membatasi bandwidth 3 Mbps per user hotspot dan 50 Mbps untuk subnet Marqiz. Firewall berhasil memblokir akses ke game online (Mobile Legends, Free Fire, PUBG, Clash of Clans) serta membatasi akses internet pada waktu shalat. Infrastruktur yang dibangun juga mampu mendukung aktivitas operasional dan live streaming dengan lebih optimal.

## PENDAHULUAN

Pemanfaatan teknologi digital telah menjadi imperatif bagi institusi di segala sektor, termasuk lembaga pendidikan dan dakwah Islam (Alhaq & Castrawijaya, 2025; Dewi, 2025; Hasmi, 2025; Karyadi, 2025; Rani, 2023). Marqiz Imam Syafi'i dan Musholla Imam Syafi'i Condet merupakan dua entitas yang aktif mengadopsi teknologi digital dalam operasionalnya, ditandai dengan rutinnnya pelaksanaan siaran langsung live streaming kajian keagamaan melalui platform YouTube. Aktivitas ini bertujuan untuk memperluas jangkauan dakwah, sekaligus memerlukan dukungan internet yang tidak hanya cepat, tetapi juga stabil dan dapat diandalkan (Fabriar, 2024; Lestari, 2024).

Namun, infrastruktur jaringan yang saat ini digunakan, yang mengandalkan koneksi berbasis Kuota (LTE), terbukti memiliki keterbatasan fundamental yang menghambat kinerja optimal (AZ et al., 2025; Fajar Rayhan Putra Irawan et al., 2025). Tantangan utama yang dihadapi meliputi: ketidakstabilan koneksi, terutama dipicu oleh faktor lingkungan seperti perubahan cuaca atau hujan lebat, yang menyebabkan kualitas live streaming dan operasional harian terganggu oleh lag dan packet loss. Selain itu, penggunaan sistem berbasis kuota juga memicu inefisiensi biaya operasional, karena konsumsi data yang tinggi cepat menghabiskan kuota yang ada, memaksa lembaga untuk terus menerus mengeluarkan biaya tak terduga (Kurniawan & Rojabi, 2026; Wibowo, 2024).

Lebih jauh, permasalahan fisik terkait cakupan juga menjadi kendala. Sinyal wireless yang dipancarkan dari modem utama memiliki cakupan Wifi yang sangat kecil, tidak mampu mencakup keseluruhan area Marqiz Imam Syafi'i dan Musholla Imam Syafi'i yang berada di gedung yang berbeda. Keterbatasan jangkauan ini membatasi pemanfaatan perangkat di berbagai lokasi dan menghambat potensi perluasan jaringan (AZ et al., 2025; Loho & Ilham, 2025; Purba et al., 2025; Sukmawati et al., 2024). Selain itu, belum terpenuhinya kebutuhan akan jaringan wired (LAN) di setiap lantai dan sistem jaringan terpisah untuk CCTV menjadi penghalang dalam aspek keamanan.

Penelitian terdahulu yang relevan antara lain dilakukan oleh Hafiz & Kurnia (2021) tentang pengembangan WLAN dan hotspot menggunakan Mikrotik di lingkungan kampus, serta Danuasmo dkk. (2023) tentang rancang bangun jaringan WLAN berbasis cloud di universitas. Namun, penelitian-penelitian tersebut masih terbatas pada lingkungan pendidikan dan belum secara spesifik membahas implementasi jaringan di lembaga dakwah dengan karakteristik kebutuhan live streaming, pembatasan akses berdasarkan waktu ibadah, serta sistem monitoring jarak jauh menggunakan DDNS. Kebaruan (novelty) penelitian ini terletak pada integrasi beberapa fitur sekaligus: (1) Quality of Service (QoS) untuk prioritas live streaming, (2) pembatasan akses game online dan pemblokiran internet pada waktu shalat, (3) konfigurasi firewall dengan fitur time-based, (4) custom port untuk winbox sebagai langkah keamanan, serta (5) sistem remote monitoring menggunakan FreeDDNS yang dikonfigurasi secara end-to-end.

Untuk menjawab kebutuhan ini, diperlukan solusi rekayasa jaringan yang mampu menyediakan kontrol penuh (granular control) dan stabilitas. Implementasi Mikrotik Router diusulkan sebagai solusi gateway utama. Mikrotik menawarkan fitur Quality of Service (QoS) yang esensial untuk memprioritaskan lalu lintas data live streaming (yang sensitif terhadap latency) dan membagi bandwidth secara adil untuk pengguna harian. Mikrotik juga dapat membuat policy dalam jaringan menggunakan fitur firewall Filter Rule, agar user jaringan

dapat dilakukan kontrol dalam mengakses jaringan, dapat juga dilakukan pembatasan akses ke web atau aplikasi tertentu sesuai dengan kesepakatan dari pihak institusi.

Lalu dalam proyek ini juga mencakup konfigurasi koneksi remote yang aman menggunakan layanan DDNS (Dynamic DNS), memungkinkan administrator untuk melakukan monitoring dan pengelolaan jaringan secara jarak jauh (remote access). Hal ini menjamin bahwa setiap gangguan dapat diatasi dengan cepat.

Berdasarkan permasalahan operasional, stabilitas, dan keterbatasan cakupan jaringan yang ada, Tugas Akhir ini bertujuan memberikan kontribusi nyata melalui implementasi solusi jaringan yang profesional dan berkelanjutan dengan judul Implementasi Infrastruktur Jaringan Internet Berbasis Mikrotik di Marqiz Imam Syafi'i & Musholla Imam Syafi'i Condet dengan Sistem Monitoring Jarak Jauh. Permasalahan utama yang diangkat mencakup penggunaan jaringan berbasis kuota, ketidakstabilan koneksi, serta keterbatasan jangkauan, sehingga penelitian ini difokuskan pada perancangan dan implementasi jaringan terintegrasi yang mampu menghasilkan koneksi stabil dan merata. Rumusan masalah meliputi bagaimana menentukan topologi jaringan dan konfigurasi router Mikrotik yang optimal, bagaimana penerapan manajemen Quality of Service (QoS) untuk menjaga stabilitas koneksi klien, bagaimana penerapan kebijakan firewall untuk membatasi akses tertentu, serta bagaimana implementasi sistem remote monitoring agar administrator dapat mengawasi dan mengelola jaringan secara efektif dari luar lokasi. Sejalan dengan itu, tujuan penelitian ini adalah mewujudkan infrastruktur jaringan yang stabil untuk mendukung kegiatan operasional dan dakwah, mengimplementasikan kebijakan firewall sesuai kebutuhan, mengoptimalkan QoS untuk menjamin kualitas layanan penting seperti live streaming, serta menghadirkan sistem monitoring jarak jauh yang efisien.

Penelitian ini memiliki relevansi dan manfaat baik secara akademis maupun praktis. Secara akademis, penelitian ini memperkaya referensi di bidang administrasi jaringan, khususnya terkait implementasi Mikrotik, QoS, manajemen bandwidth, firewall, serta remote monitoring pada lingkungan nyata yang jarang dibahas seperti masjid atau lembaga dakwah. Selain itu, penelitian ini dapat menjadi referensi lanjutan, memperkaya literatur, meningkatkan pemahaman konsep jaringan secara terintegrasi, serta menjadi model pembelajaran praktis bagi mahasiswa. Dari sisi praktis, hasil penelitian ini memberikan panduan teknis yang dapat langsung diterapkan oleh administrator jaringan, membantu meningkatkan stabilitas layanan live streaming, meningkatkan efisiensi biaya melalui penggunaan internet fiber, serta memperkuat keamanan lingkungan melalui integrasi CCTV. Implementasi sistem VPN/DDNS juga memberikan kemudahan monitoring dan manajemen jaringan secara jarak jauh, sementara desain jaringan yang dihasilkan dapat diadopsi oleh lembaga lain seperti masjid, sekolah, atau yayasan yang membutuhkan infrastruktur jaringan handal dengan biaya terjangkau.

## **METODE PENELITIAN**

Penelitian ini menggunakan pendekatan penelitian terapan (applied research) dengan metode deskriptif dan eksperimental. Pendekatan ini dipilih karena penelitian berfokus pada penyelesaian masalah nyata di lapangan melalui penerapan langsung sistem jaringan. Metodologi yang digunakan dirancang agar setiap tahap, mulai dari perancangan, konfigurasi, hingga evaluasi jaringan, dapat dilakukan secara terstruktur dan menghasilkan temuan yang dapat dipertanggungjawabkan.

### **Studi Literatur dan Benchmarking (Literature Review)**

Pada tahap awal, peneliti mengumpulkan berbagai referensi yang berkaitan dengan administrasi jaringan, manajemen bandwidth (QoS), firewall, Hotspot Mikrotik, integrasi CCTV, serta teknologi VPN/DDNS. Referensi ini diambil dari berbagai buku jaringan, jurnal, serta penelitian terdahulu. Tujuannya adalah memahami konsep dan best practices yang akan menjadi dasar dalam proses perancangan dan implementasi jaringan di lokasi penelitian.

### **Analisis Lingkungan, Identifikasi Permasalahan, dan Pengumpulan Data Lapangan**

Setelah memahami konsep dasar, peneliti melakukan pengamatan langsung di lokasi penelitian untuk melihat kondisi jaringan yang sudah berjalan, kendala yang muncul, serta kebutuhan yang disampaikan oleh pengelola. Data yang dikumpulkan mencakup topologi jaringan, kapasitas internet, perangkat yang digunakan, jumlah pengguna, dan pola penggunaan bandwidth. Peneliti juga mencatat beberapa masalah utama seperti ketidakstabilan live streaming, penggunaan kuota yang kurang efisien, integrasi CCTV yang belum optimal, dan kebutuhan layanan Hotspot yang lebih teratur.

### **Penetapan Kriteria Evaluasi Sistem**

Untuk menilai keberhasilan implementasi jaringan, peneliti menetapkan beberapa kriteria evaluasi yang digunakan sebagai acuan. Kriteria ini mencakup aspek teknis dan operasional agar hasil yang diperoleh dapat dinilai secara menyeluruh. Indikator yang digunakan meliputi stabilitas live streaming, pembagian bandwidth setelah penerapan QoS, penyesuaian policy jaringan melalui fitur firewall pada mikrotik, kemudahan pengelolaan dengan VPN/DDNS, serta performa layanan Hotspot dan CCTV. Penetapan kriteria ini membantu memastikan apakah solusi yang diterapkan sudah sesuai dengan tujuan penelitian atau masih perlu penyesuaian.

### **Implementasi Rancangan dan Pengujian Sistem Secara Bertahap**

Tahap implementasi dilakukan berdasarkan hasil analisis dan rancangan yang telah dibuat sebelumnya. Konfigurasi dilakukan secara bertahap, mulai dari pengaturan dasar Router, DHCP, dan IP address, kemudian dilanjutkan ke bagian yang lebih detail seperti QoS, firewall, Hotspot, integrasi CCTV, serta pengaturan VPN/DDNS. Setelah seluruh konfigurasi diterapkan, peneliti melakukan pengujian untuk melihat perbedaan kinerja jaringan sebelum dan sesudah implementasi. Pengujian dilakukan dengan memantau performa live streaming, mengukur penggunaan bandwidth, mencoba login dan pembatasan akses pada Hotspot, mengecek kualitas CCTV, serta menguji akses jarak jauh melalui VPN/DDNS. Seluruh hasil pengujian akan di dokumentasikan agar dapat dianalisis lebih lanjut, termasuk jika ditemukan kendala selama proses implementasi. Dengan cara ini, peneliti dapat melihat seberapa besar perubahan yang terjadi setelah konfigurasi baru diterapkan.

### **Rekomendasi**

Pada tahap akhir, peneliti menyusun rekomendasi berdasarkan hasil implementasi dan evaluasi. Rekomendasi ini mencakup langkah-langkah teknis yang dapat dilakukan pengelola untuk menjaga kestabilan jaringan, seperti pengaturan bandwidth ideal, pengaturan policy pada fitur firewall, pengelolaan user Hotspot, dan perencanaan peningkatan kapasitas jaringan di masa mendatang. Selain itu, peneliti merangkum berbagai pembelajaran penting yang diperoleh selama proses penelitian. Pembelajaran ini dapat menjadi pedoman bagi mahasiswa, praktisi jaringan, atau lembaga lain yang ingin membangun sistem jaringan dengan karakteristik serupa. Dengan demikian, penelitian ini tidak hanya memberikan solusi untuk

kasus tertentu, tetapi juga menawarkan kontribusi yang lebih luas bagi pengembangan sistem jaringan di lingkungan pendidikan dan dakwah

## HASIL DAN PEMBAHASAN

### Implementasi Sistem

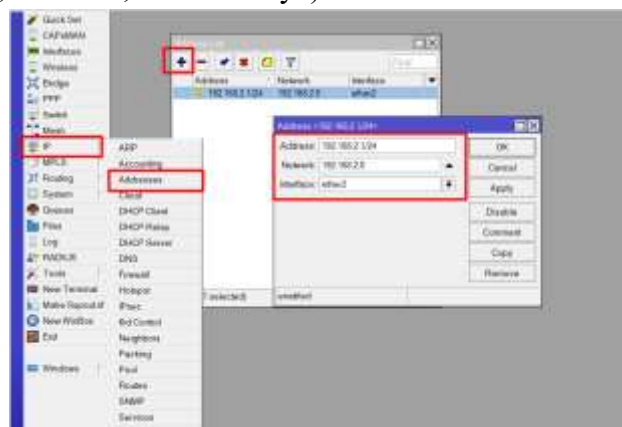
Pada tahap implementasi, dilakukan proses konfigurasi jaringan sesuai dengan rancangan yang telah dibuat sebelumnya. Tujuan dari tahap ini adalah untuk membangun sistem jaringan yang dapat berjalan dengan stabil, mudah dikelola, serta mampu mendukung kebutuhan operasional di lingkungan Marqiz Imam Syafi'i dan Musholla Imam Syafi'i Condet.

Proses implementasi dilakukan secara bertahap, dimulai dari konfigurasi dasar hingga penerapan fitur-fitur lanjutan seperti manajemen *bandwidth*, *firewall*, serta sistem *remote monitoring*. Setiap langkah konfigurasi didokumentasikan dalam bentuk *capture* untuk memberikan gambaran nyata terkait proses yang dilakukan.

### Konfigurasi Dasar Mikrotik

Pada tahap awal implementasi, dilakukan konfigurasi dasar pada Mikrotik sebagai pusat pengelolaan jaringan, dengan melakukan konfigurasi *User login*, *IP Address*, *DHCP Server*, *DHCP Client* ke Modem Provider serta *NAT* agar jaringan lokal dapat terhubung ke internet. *Router* ini juga berfungsi sebagai *gateway* bagi seluruh perangkat yang terhubung dalam jaringan.

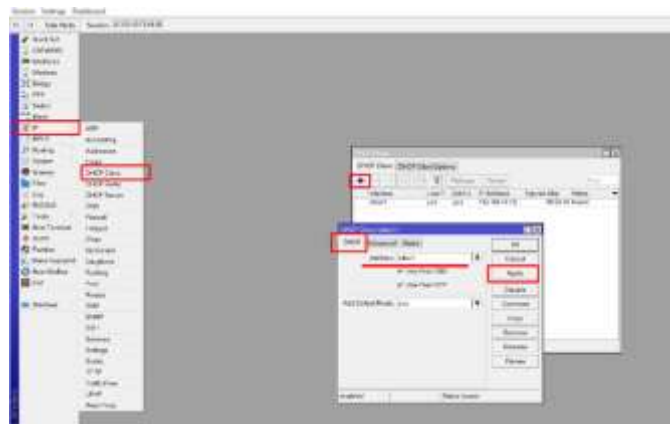
Konfigurasi *IP Address* pada Mikrotik, pilih menu *IP > Addresses > + add baru >* isikan data IP nya (*Interface*, *Network*, *IP Address*nya)



Gambar 1, Konfigurasi IP Address ke Ether 2

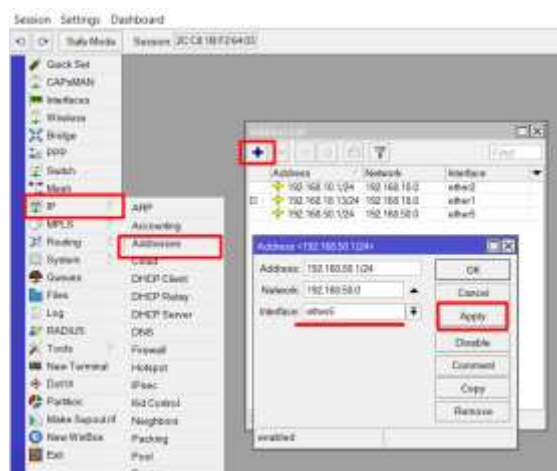
Berikutnya kita bisa lakukan konfigurasi *IP DHCP Client* mengarah ke modem provider di ether1 dan IP untuk ether5 pada Mikrotik mengarah ke Marqiz Imam Syafi'I, media transmisi yang digunakan untuk menyambungkan Musholla Imam Syafi'I Condet dan Marqiz Imam Syafi'I Condet menggunakan kabel *fiber* optik dan menggunakan perangkat HTB, sebagai perangkat untuk mengkonvert data dari kabel *LAN* ke kabel *Fiber*.

Konfigurasi *DHCP Client*, *IP > DHCP Client > add (+) >* pilih *interface* ether1, lalu centang *Used Peer DNS* dan *Use Peer NTP*, pada kolom *Add Default Route* pilih *yes > Apply*



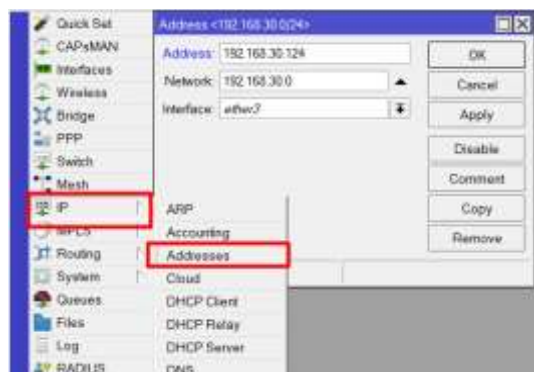
**Gambar 2, Konfigurasi IP *DHCP Client* Pada Ether1**

Jika sudah, maka nanti kita akan mendapatkan IP *DHCP* yang di berikan dari modem provider, setelah tahap ini *router* Mikrotik sudah bisa terkoneksi ke internet, berikutnya kita bisa lakukan konfigurasi IP untuk mengarah ke ether5 yaitu *interface* yang mengarah ke Marqiz Imam Syafi'I Condet. Ke menu IP > *Addresses* > add (+) > isikan IP nya dan *interface* diarahkan ke ether5.



**Gambar 3, Konfigurasi IP Address ke Ether5**

Selanjutnya kita akan lakukan konfigurasi di ether3 sebagai koneksi *wifi hotspot* untuk jamaah Musholla Imam Syafi'I Condet, ke menu IP > *Addresses* > add (+) > isikan IP nya dan pada bagian *interface* diarahkan ke ether3.



**Gambar 4, Konfigurasi IP Address ke Ether3 Untuk *Hotspot***

Selanjutnya kita akan konfigurasi user *login* Mikrotik, kita akan membuat 2 akun *user login* untuk mengakses Mikrotik, 1 akun *read only*, 1 akun *full access*, nantinya akun *read only*

ini akan di *share* kepada pihak DKM, jika dari pihak DKM ingin mengakses Mikrotik sembari melakukan pengecekan penggunaan jaringan. Konfigurasi user *read only*, pilih menu *System > Users > add (+) >* pada bagian *name*, isikan *name* nya muis, dan di bagian *password* isikan *password* nya.



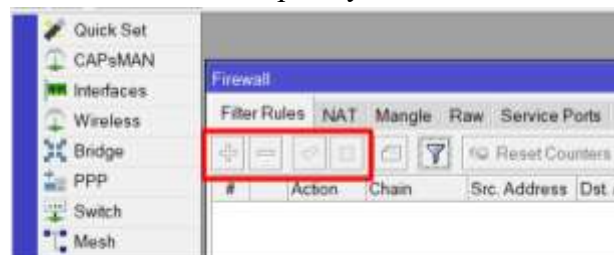
**Gambar 5, Konfigurasi User *ReadOnly* untuk DKM**

Lalu kita buat untuk user *full access* nya, untuk tahap konfigurasinya hampir sama, kita tentukan *username/password*, pada kolom *Group* pilih *Full*, akun *full access* ini merupakan *group* yang diberikan izin untuk ke semua, mulai dari menambahkan konfigurasi, menghapus, atau hanya melihat konfigurasi.



**Gambar 6, Konfigurasi User *Full Access* untuk Administrator jaringan**

Saat kita *login* dengan akun *group ReadOnly*, akun ini tidak bisa menambahkan atau menghapus konfigurasi, tombol tambah dan hapus nya tidak bisa di klik,



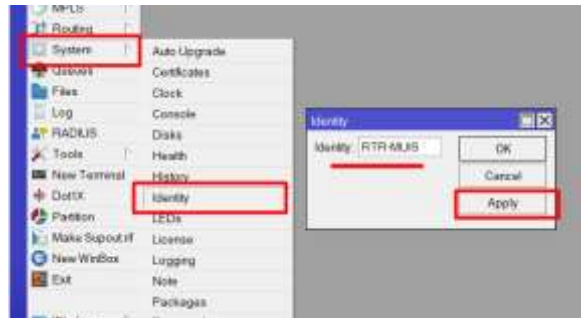
**Gambar 7, Akses Mikrotik Menggunakan User *ReadOnly***

Berbeda saat kita *login* dengan akun *group Full*, akun ini bisa menambahkan, menghapus konfigurasi, *disable enable rule*, tombol ketika menggunakan akun *readonly* tidak bisa di klik, saat menggunakan akun dengan *group full*, tombol bisa di klik.



**Gambar 8, Akses Mikrotik Menggunakan User *Full Access***

Terlihat pada gambar, tombol *add (+)*, bisa di klik, dan kita bisa menambahkan konfigurasi. Selanjutnya kita ingin mengganti nama pada *router* Mikrotik, sebagai identitas *router* milik kita, disini kita akan berikan nama *router* dengan RTR-MUIS. Pada menu *System* > *Identity* > Isikan penamaan *identity* nya sesuai dengan kebutuhan > RTR-MUIS > *Apply*



**Gambar 9, Konfigurasi *Identity* Router Mikrotik.**

Selain sebagai penanda *router*, *identity* ini berguna juga membantu administrator jaringan ketika dalam kondisi banyak *router* yang diakses, sehingga tidak mudah tertukar *router* mana yang sedang di *remote*.

Langkah Berikutnya kita melakukan konfigurasi *DHCP Server*, berfungsi agar *client* jaringan tidak perlu melakukan konfigurasi IP pada perangkat mereka secara manual, dan hanya perlu terkoneksi pada *Wifi* dan *LAN* maka *client* bisa terhubung ke jaringan karena mendapatkan IP otomatis dari Mikrotik.



**Gambar 10, Konfigurasi *DHCP Server* pada ether2**



**Gambar 11, Konfigurasi *DHCP Server* pada ether5**

Konfigurasi *DHCP Server* pada Mikrotik, pilih menu *IP* > *DHCP Server* > *DHCP Setup* > pilih *Interface* ether yang ingin dijadikan sebagai *DHCP Server* > isikan IP *network* pada *interface* > masukan *gateway* > pilih *range* IP yang ingin di berikan > *DNS Servers* > *lease time*. Jika ingin simpel, teman teman tinggal *next* sampai akhir setelah pemilihan *interface* dan sudah dilakukan konfigurasi IP, Mikrotik akan otomatis secara *default* mengikuti sesuai *range* IP berapa yang di berikan dari segmentasi IP nya lalu IP *network* nya > *gateway* IP nya.

Jika sudah dilakukan konfigurasi *DHCP*, kita bisa melihat client IP *DHCP* pada menu *IP* > *DHCP Server* > *leases*

| Address        | MAC Address       | ClientID           | Server | Address        | MAC Address       | ClientID | Server |
|----------------|-------------------|--------------------|--------|----------------|-------------------|----------|--------|
| 192.168.10.48  | 6A:A2:00:F5:29:4C | 134.A2.0E.3D.4C    | dhcp1  | 192.168.10.48  | 6A:A2:00:F5:29:4C |          |        |
| 192.168.10.49  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.49  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.50  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.50  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.51  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.51  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.52  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.52  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.53  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.53  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.54  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.54  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.55  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.55  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.56  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.56  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.57  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.57  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.58  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.58  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.59  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.59  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.60  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.60  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.61  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.61  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.62  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.62  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.63  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.63  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.64  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.64  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.65  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.65  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.66  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.66  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.67  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.67  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.68  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.68  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.69  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.69  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.70  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.70  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.71  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.71  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.72  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.72  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.73  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.73  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.74  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.74  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.75  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.75  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.76  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.76  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.77  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.77  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.78  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.78  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.79  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.79  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.80  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.80  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.81  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.81  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.82  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.82  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.83  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.83  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.84  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.84  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.85  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.85  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.86  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.86  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.87  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.87  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.88  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.88  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.89  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.89  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.90  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.90  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.91  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.91  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.92  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.92  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.93  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.93  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.94  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.94  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.95  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.95  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.96  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.96  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.97  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.97  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.98  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.98  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.99  | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.99  | 8E:1D:67:A6:A3:1E |          |        |
| 192.168.10.100 | 8E:1D:67:A6:A3:1E | 13a.1d.67.a6.a3.1e | dhcp1  | 192.168.10.100 | 8E:1D:67:A6:A3:1E |          |        |

Gambar 12, List *Client IP DHCP* Mikrotik

Agar *client* jaringan juga dapat terkoneksi ke internet, kita akan melakukan konfigurasi *NAT*. Konfigurasi *NAT* pada *router* Mikrotik, pilih menu *IP > Firewall > NAT > add (+) >* isi pada kolom *Chain* pilih *srcnat >* isi *Out Interface*, *Interface* yang mengarah ke internet atau modem provider (*ether1*) > pilih menu *action* dibagian atas > dan isikan kolom *action* pilih *masquerade*



Gambar 13, Konfigurasi *NAT* Mikrotik



Gambar 14, Konfigurasi *NAT* Mikrotik *Masquerade*

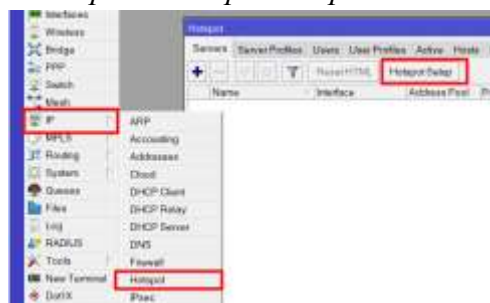
Dan untuk pengecekan *NAT* nya, kita bisa langsung pengetesan pada *client* jaringan, dan kita lihat pada *rule NAT* nya pastikan sudah *counting* ada paket yang lewat.

| File Name | Chain  | Out    | Service Ports | Connection | Address List | Layer/Protocol |
|-----------|--------|--------|---------------|------------|--------------|----------------|
| +         | srcnat | ether1 |               |            |              |                |

Gambar 15, *Counting* Paket *Rule NAT*

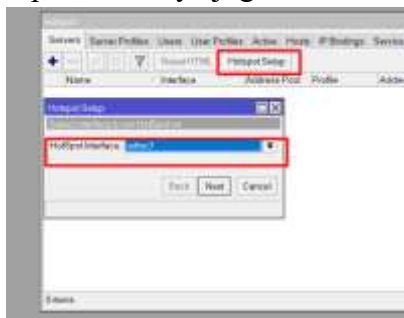
## Konfigurasi *Hotspot*

Berikutnya kita lanjutkan untuk melakukan konfigurasi *hotspot*, ada 2 jenis *wifi* di Musholla Imam Syafi'I, *wifi* pertama *wifi* khusus DKM Muis, dan *wifi* kedua bisa digunakan semua jamaah, *wifi* untuk jamaah menggunakan sistem *hotspot*, sehingga jamaah yang ingin terkoneksi di perlukan *login* terlebih dahulu untuk terhubung ke internet. Langkah konfigurasinya, pilih menu *IP > Hotspot > Hotspot Setup*.

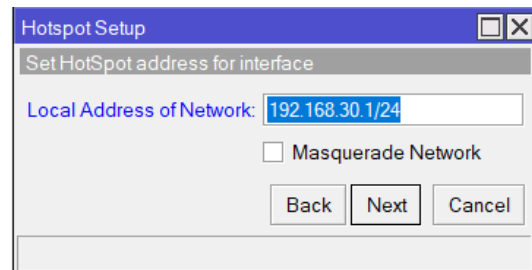


Gambar 16, Konfigurasi *Hotspot Setup*

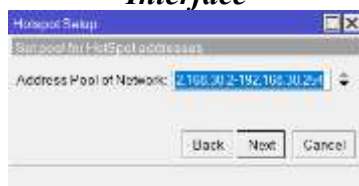
Ketika *Hotspot Setup* di klik, nanti akan muncul untuk konfigurasi lanjutan untuk *hotspot* nya. Pilih *Interface* mana sebagai koneksi *hotspot* (ether3) lalu *next* > isikan IP *gateway* nya pada bagian *Local Address of Network*, lalu *next* > kita bisa *custom* untuk *pool* IP yang akan di berikan pada bagian *Address Pool of Network*, namun bisa juga mengikuti *default* IP *pool* nya sesuai segmentasi IP, lalu *next* > *Select Certificate*, *next* aja > bagian IP *Address of SMTP Server*, lanjut *next* aja > pada bagian *DNS Server*, sesuaikan *DNS Server* nya yang ingin di gunakan, bisa gunakan *DNS* provider internet, atau menggunakan *DNS* google, 8.8.8.8, lalu *next* > berikutnya *DNS Name*, *DNS name* ini nanti sebagai *DNS URL* saat kita *login hotspot* nya, bisa kita *custom* sesuai keinginan, disini kita akan isi muis.net, lalu *next* > tahap ini kita akan buat user *hotspot*, ditahap ini kita bisa *custom* dalam pengisian *user* dan *password*, kita bisa gunakan *user* dan *password* sesuai kenginan dan kebutuhan, disini kita akan isi user nya muis dan password nya juga muis, lalu *next* lagi dan selesai.



**Gambar 17, Konfigurasi Hotspot Interface**



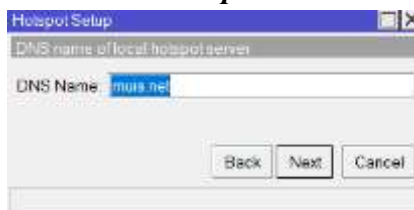
**Gambar 18, Konfigurasi IP pada Interface Hotspot**



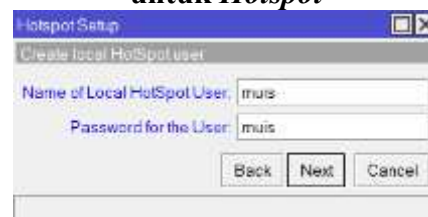
**Gambar 19, Konfigurasi IP Pool untuk Hotspot**



**Gambar 20, Konfigurasi DNS Server untuk Hotspot**

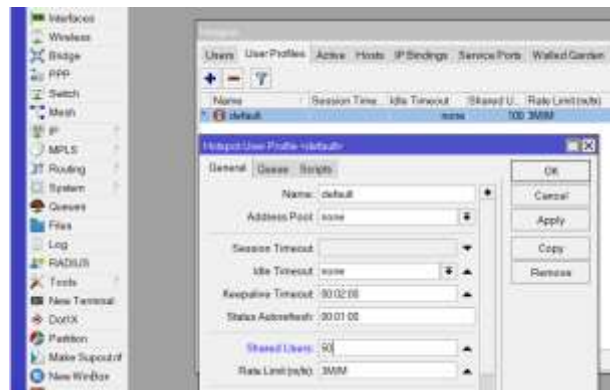


**Gambar 21, Konfigurasi DNS Name Hotspot**



**Gambar 22, Konfigurasi User Hotspot**

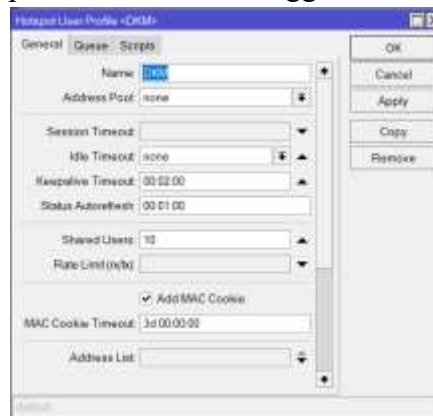
Jika sudah terbuat *hotspot* nya, berikutnya kita akan konfigurasi untuk limitasi *bandwith* user *hotspot* nya. Kita bedakan dulu *profile* limitasinya, untuk DKM dan untuk jamaah, untuk *profile* DKM tidak kita lakukan limitasi, namun untuk profil jamaah kita limit 3MB per user. Langkah konfigurasinya pilih menu *User Profile* pada *Hotspot*



**Gambar 23, User Profile Hotspot Jamaah**

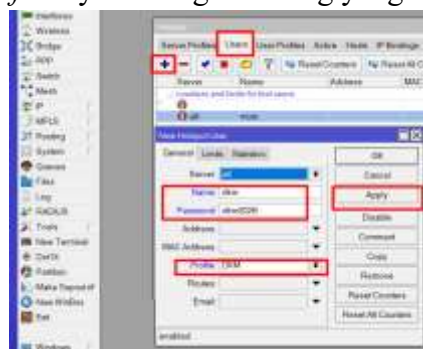
Di menu ini, kita akan berikan pada bagian *shared user* 50, yang nantinya dengan 1 akun user *hotspot* bisa digunakan bersamaan sebanyak 50 pengguna, pada bagian *Rate Limit (rx/tx)*, kita limit 3MB, maka per pengguna user akan dilimitasi sebesar 3MB.

Selanjutnya kita buat User Profile untuk DKM, tidak ada limitasi *bandwith* untuk User Profiles DKM, pada bagian Rate limit (rx/tx) kita kosongkan saja, dan untuk bagian *Shared Users* kita isikan 10 saja, karena pihak DKM bisa menggunakan *wifi* khusus DKM.



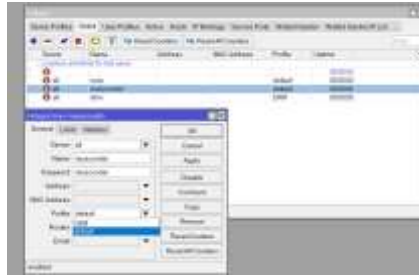
**Gambar 24, User Profile Hotspot DKM**

Berikutnya ke menu *users*, disini kita akan membuat user untuk jamaah dan DKM, lalu kita masukan user tersebut ke *profile* nya masing – masing yang sebelumnya sudah kita buat.



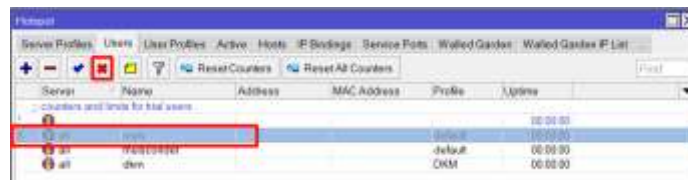
**Gambar 25, Membuat User Hotspot DKM**

Pilih *Users > add (+)* > pada kolom *name* dan *password*, isikan *username* dan *password* user *hotspot* nya, untuk user *hotspot* DKM, kita akan menggunakan *dkm* sebagai *username* nya, dan *dkm2026!* untuk *password* nya, lalu masukan user *dkm* ini di *profile* DKM yang telah kita buat. Berikutnya kita buat untuk jamaah, dengan *username* dan *password* muiscondet, kita samakan agar mempermudah jamaah saat *login*.



**Gambar 26, Membuat User *Hotspot* Jamaah**

Cara konfigurasi nya hampir sama seperti untuk user DKM, namun untuk jamaah kita bedakan di kolom *Profile*, kita pilih *Profile default*, karena untuk *Profile hotspot* jamaah kita menggunakan *profile default*. Jika sudah, maka user *hotspot* sudah berhasil kita buat, kita bisa menonaktifkan user *hotspot* awal ketika kita melakukan konfigurasi *hotspot*, karena tidak di gunakan, atau bisa kita *remove* user nya. Caranya kita klik user nya, lalu kita pilih bisa *disable* (X) atau *remove* (-).



**Gambar 27, Disable User *Hotspot***

Selanjutnya kita akan melakukan percobaan akses melalui *wifi hotspot*, melakukan *browsing* dan *speedtest* memastikan *bandwith* jamaah sudah terlimit sesuai dengan *profile* yang telah di buat. Untuk melakukan pengecekan user *hotspot*, pada menu *hotspot > Active*.

### Konfigurasi Limitasi *Bandwidth*

Pada tahap ini dilakukan pembatasan *bandwidth* sebesar 50 *Mbps* untuk jaringan 192.168.50.0/24. Segment tersebut untuk jaringan Marqiz Imam Syafi'I Condet. Langkah konfigurasi nya pilih menu *Queues > Pada Tab Simple Queues > add (+) > Name* nya isikan nama *queue* yang ingin dibuat, disini kita namakan Limit Marqis > Pada bagian Target, isikan IP yang ingin di batasi (192.168.50.0/24) > lalu pada bagian *Max Limit*, masukan Target Upload 50M dan Target Download 50M > lalu *Apply*.



**Gambar 28, Konfigurasi *Queue Segment* Marqiz Imam Syafi'I Condet**

Setelah dilakukan pembatasan *bandwidth* maka hasil ketika kita lakukan tes *speed* pada platform *speedtest*, segment IP 192.168.50.0/24 berhasil dibatasi.

### Konfigurasi *Firewall* Pembatasan Akses User

Kita lakukan pembatasan akses pada user jaringan melalui fitur *firewall* di Mikrotik, ini berguna agar user jaringan dalam mengakses internet tetap mengikuti *policy* jaringan yang di

berikan oleh pihak DKM. pembatasan akses internet dengan melakukan pemblokiran terhadap beberapa *game online* dan pembatasan akses internet pada waktu shalat.

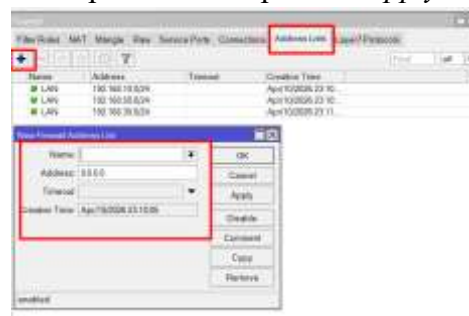
Pada tahap pertama dilakukan pembatasan akses terhadap *game online*. Adapun *game* yang diblokir meliputi *Mobile Legends*, *Free Fire*, *PUBG*, dan *Clash of Clans*, yang merupakan *game* dengan jumlah pengguna yang cukup tinggi. Untuk konfigurasi nya pilih menu IP > Firewall > Filter Rules > add (+) > Di menu Chain pilih *forward* > pada kolom *Protocol* pilih protokol apa yang ingin di blokir *TCP* atau *UDP* > pada kolom *Dst Port*, diisikan port yang digunakan *game online* yang akan diblokir > Pada tab *Action* > lalu *Action* nya pilih *drop*. Kita bisa tambahkan *comment* pada *rule* sebagai keterangan. Pada *rule* nya kita klik kanan, dan pilih *Comment*, dan isikan *comment* yang diinginkan.

Untuk mengetahui port yang di gunakan *game online* tersebut, kita dapat mencari referensi yang tersedia di internet. Untuk referensi disini saya menggunakan referensi dari bilhanet merupakan penggiat di bidang jaringan komputer yang sering membagikan informasi dan referensi teknis.[51].



**Gambar 29, Konfigurasi Firewall Blokir Game**

Selanjutnya kita akan mencoba melakukan pembatasan akses internet di waktu shalat, ketika waktu shalat tiba, internet di matikan. Langkah awal kita buat list IP untuk LAN, kita bisa memanfaatkan fitur *Address Lists* untuk mengelompokkan segmentasi IP di 1 profil. Ke menu *firewall* > *Address Lists* > *add (+)* > di kolom *name*, isikan nama profil nya, pada bagian *address* isikan IP yang ingin di kelompokkan dalam profil > *Apply*



**Gambar 30, Pengelompokan IP menggunakan Address Lists**

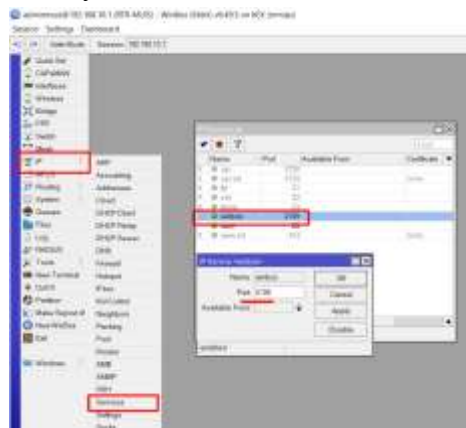
Selanjutnya kita buat *rule firewall* nya, kita memanfaatkan fitur *time* untuk penentuan waktu otomatis *rule* nya bekerja, selain di waktu itu *rule* non aktif sendirinya. Pada menu *firewall* > *add (+)* > pada bagian *Chain*, pilih *forward* > *Advanced* > *Src. Address List*, masukan *Address list* yang sudah di buat sebelumnya dengan nama *LAN* > pilih tab *extra*, pada bagian *time* isikan waktu dan hari apa saja *rule* bekerja > ke tab *action*, lalu pilih *action drop*. Kita juga berikan *comment* sebagai keterangan. *Rule* ini di sesuaikan dalam 5 waktu shalat.



**Gambar 31, Penggunaan Fitur *Time* Pada *Firewall* Mikrotik Konfigurasi *Disable Port* Yang Tidak Digunakan Dan *Custom Port Winbox***

Secara *default*, Mikrotik memiliki beberapa *service* yang aktif seperti *Telnet*, *FTP*, *SSH*, *WWW*, dan *Winbox*. Namun, tidak semua *service* tersebut digunakan dalam implementasi ini. Oleh karena itu, *service* yang tidak diperlukan akan dinonaktifkan untuk mengurangi celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Selain itu, dilakukan juga perubahan port *default* pada *winbox* menggunakan port 8291, namun pada implementasi ini port diubah menjadi 2109. Ke menu *IP > Services > klik winbox*, pada kolom port masukan port yang ingin diubah > lalu *Apply*. Dan untuk menonaktifkan *service* lain, kita klik saja *service* nya, lalu > *disable*



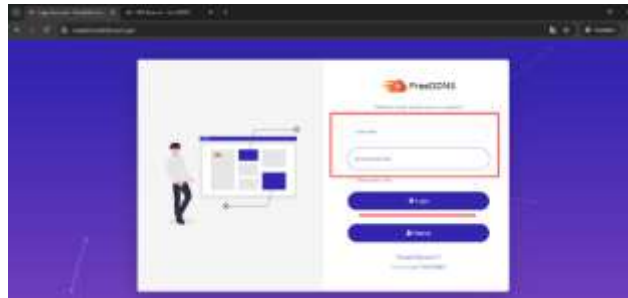
**Gambar 32, *Custom Port Winbox* dan *Disable Service* Konfigurasi *Remote Monitoring Jarak Jauh***

Berikutnya kita akan melakukan konfigurasi akses *remote monitoring* jarak jauh pada perangkat Mikrotik dengan memanfaatkan layanan *Dynamic DNS (DDNS)* dari *FreeDNS*. Penggunaan *DDNS* ini bertujuan untuk mengatasi keterbatasan alamat IP publik yang bersifat dinamis, maupun kondisi di mana pihak *ISP* tidak memberikan IP publik secara langsung kepada pelanggan.

Pada beberapa kasus, *ISP* hanya memberikan alamat IP *private* di sisi pelanggan, sehingga perangkat tidak dapat diakses langsung dari jaringan luar. Selain itu, terdapat juga kondisi di mana *ISP* memberikan IP publik pada perangkat modem pelanggan, namun alamat tersebut bersifat dinamis dan dapat berubah sewaktu-waktu. Hal ini menyebabkan akses *remote* menjadi tidak stabil apabila hanya mengandalkan alamat IP secara langsung.

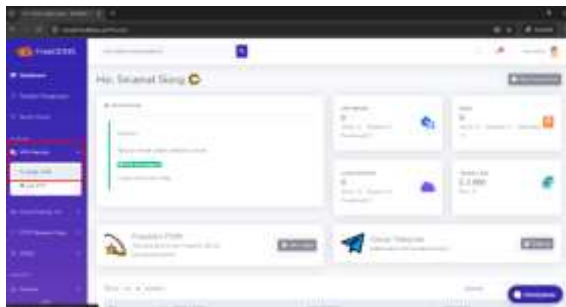
Dengan adanya layanan *DDNS*, perubahan alamat IP tersebut dapat diatasi karena *domain* yang digunakan akan secara *otomatis* diperbarui mengikuti IP publik terbaru. Sehingga, perangkat Mikrotik tetap dapat diakses secara konsisten menggunakan *domain* yang telah ditentukan.

Langkah awal konfigurasi, kita akses terlebih dahulu untuk *website FreeDDNS* nya, jika belum memiliki akun dapat membuat akun terlebih dahulu dengan mengklik *Signup*, dan mengisi data yang di minta,

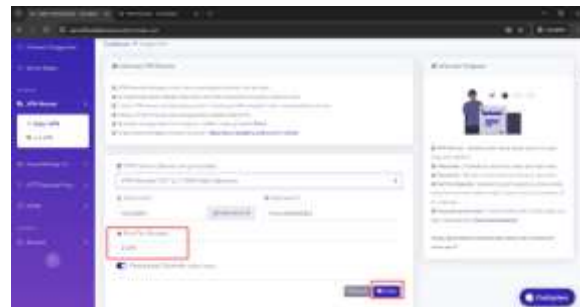


**Gambar 33, Login Website FreeDDNS**

Jika sudah *login* berikutnya, kita ke menu *VPN Remote > Order VPN*, untuk melakukan pembelian akses akun *VPN* nya. *FreeDDNS* memberikan 1 akses gratis dalam pembuatan *VPN* nya, bagi akun yang baru terdaftar di *web FreeDDNS*. Nantinya kita dapat melakukan *topup* untuk *order VPN* pada periode selanjutnya, dikarenakan akun *VPN* akan *expired* selama 1 bulan.



**Gambar 34, FreeDDNS Pembelian VPN**



**Gambar 35, FreeDDNS Pembuatan VPN Remote Akses**

Berikutnya, pada halaman *Order VPN*, dilakukan pemilihan server *VPN* yang akan digunakan. Pada bagian *VPN Server*, dipilih server yang berlokasi di Indonesia agar koneksi yang dihasilkan lebih stabil dan memiliki *latency* yang lebih rendah.

Selanjutnya, pada bagian *username* dan *password*, isikan sesuai yang kita inginkan, pada bagian *port*, masukkan *port* yang akan digunakan untuk akses *remote*. *Port* ini adalah *port winbox* pada Mikrotik. Secara *default*, *winbox* menggunakan *port 8291*, namun pada Mikrotik nya kita telah ubah menjadi *2109* sebagai salah satu langkah peningkatan keamanan. Jika sudah klik *Order*, dan pilih menu *List VPN*.

Nanti akan ada 1 akun *vpn* yang telah kita buat, lalu kita klik *manage*, dan akan keluar informasi *VPN* kita, kita bisa langsung *copy script* yang tersedia di bagian *Configuration*, dan kita paste kan di Mikrotik.

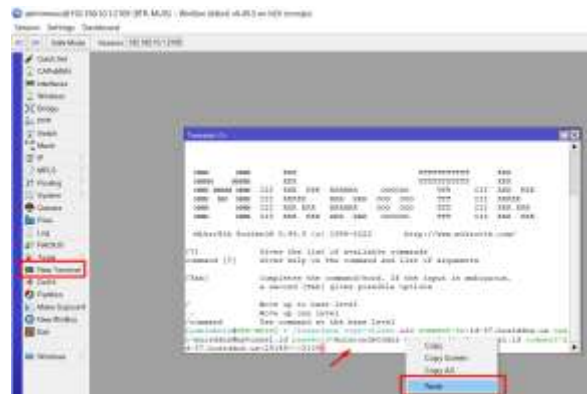


**Gambar 36, FreeDDNS List VPN**



**Gambar 37, FreeDDNS Configuration Script**

Pada keterangan informasi *VPN*, terdapat kolom *URL Remote*, nantinya *URL* ini yang akan di gunakan untuk akses mikrotik dari luar jaringan, jika *script* konfigurasi sudah di *paste* pada Mikrotik



**Gambar 38, Paste Konfigurasi FreeDDNS ke Mikrotik**

Jika sudah *paste*, kita lakukan percobaan akses dari luar, *logout winbox* nya, dan koneksi kan kembali *Wifi* menggunakan internet selain dari jaringan Mikrotik, disini kita percobaan menggunakan internet *hotspot* pribadi dari HP



**Gambar 39, Akses Mikrotik dari luar jaringan**

Pada bagian *Connect to* isikan *URL* yang tertera pada *web FreeDDNS* sebelumnya, lalu *login* dan *password* menggunakan user yang sudah di buat pada Mikrotik, kemudian klik *Connect*.



**Gambar 40, Berhasil Akses Mikrotik dari Luar jaringan**

Dan kita bisa mengakses Mikrotik kita, meskipun dari luar jaringan, pada *Interface List* terdapat 1 list *interface VPN* yang telah berhasil terbuat dari statusnya *running*, karena kita telah masukan konfigurasi *VPN* nya melalui *script* konfigurasi yang di berikan pada *web FreeDDNS*.

### Konfigurasi *DVR CCTV*

Untuk infrastruktur *CCTV* pada Marqiz Imam Syafi'i dan Musholla Imam Syafi'i Condet di implementasikan oleh vendor terkait, mulai dari pemasangan, penjaluran kabel, dan instalasi *DVR* dan *CCTV* nya, namun saya membantu untuk melakukan konfigurasi umum pada *DVR* seperti *IP Address*, Tanggal dan waktu pada *DVR*. Untuk *IP Address* mengikuti segment 192.168.10.x, dengan *IP DVR* 192.168.10.99/24, lalu untuk *timezone* pilih (*GMT+0700*).



Gambar 41, Konfigurasi IP pada *DVR*



Gambar 42, Konfigurasi *Time Zone DVR*



Gambar 43, Tampilan Monitor *CCTV*

### Pengujian Sistem

Pengujian sistem dilakukan untuk mengetahui sejauh mana implementasi jaringan yang telah dilakukan mampu menyelesaikan permasalahan yang terjadi sebelumnya. Proses pengujian ini mencakup beberapa aspek, yaitu stabilitas jaringan, manajemen *bandwidth*, keamanan akses, serta kemampuan *remote monitoring*. Pengujian dilakukan dengan membandingkan kondisi jaringan sebelum dan sesudah implementasi.

#### Kondisi Sebelum Implementasi

Sebelum dilakukan implementasi, kondisi jaringan di Marqiz Imam Syafi'i dan Musholla Imam Syafi'i Condet masih belum optimal. Koneksi internet yang digunakan masih berbasis kuota (*LTE*), sehingga sering mengalami ketidakstabilan. Hal ini berdampak pada aktivitas jaringan, yang masih sering mengalami *buffering* dan *latency* yang tinggi.

Selain itu, belum adanya manajemen jaringan sehingga jaringan tidak bisa di monitor dan dilakukan kontrol terkait penggunaan nya.

Tabel 1 Tabel Kondisi Jaringan Sebelum Implementasi

| No | Aspek             | Kondisi Sebelum Implementasi                                                                                                                           |
|----|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Sumber Internet   | Menggunakan jaringan <i>LTE</i> (kuota) yang cenderung tidak stabil.                                                                                   |
| 2  | Performa Jaringan | Sering terjadi <i>latency</i> tinggi dan <i>buffering</i> saat digunakan secara bersamaan, lokasi sumber <i>wifi</i> hanya di sekitar modem orbit saja |

|   |                            |                                                                             |
|---|----------------------------|-----------------------------------------------------------------------------|
| 3 | Manajemen <i>Bandwidth</i> | Belum ada pembagian <i>bandwidth</i> , sehingga penggunaan tidak terkontrol |
| 4 | Keamanan Jaringan          | Tidak ada pembatasan akses, seluruh pengguna bebas mengakses internet       |
| 5 | Monitoring Jaringan        | Tidak ada <i>monitoring</i> pada jaringan                                   |

Untuk memperkuat kondisi tersebut, dilakukan pengujian awal, dengan mencoba menjalankan *speedtest* dan melakukan akses ke *youtube*

Dalam mengakses layanan seperti *YouTube* dan melakukan pengujian menggunakan *speedtest*, koneksi internet terasa lambat. Meskipun pada akhirnya masih dapat diakses, proses pemuatan konten membutuhkan waktu yang cukup lama sehingga mengganggu kenyamanan pengguna. Dalam pengetesan *ping* juga terlihat tidak stabil untuk *latency* nya.

### Kondisi Setelah Implementasi

Setelah dilakukan implementasi infrastruktur jaringan dengan menggunakan perangkat Mikrotik sebagai manajemen nya, kondisi jaringan mengalami peningkatan yang signifikan baik dari sisi performa, keamanan, maupun pengelolaan. Perubahan kondisi jaringan setelah implementasi dapat dilihat pada Tabel 4.2 berikut.

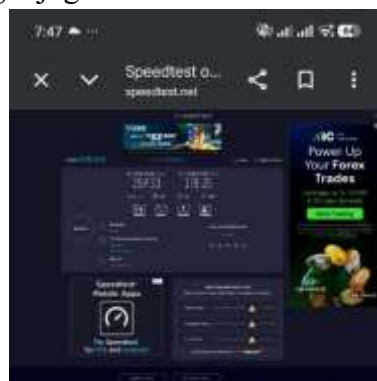
**Tabel 1, Tabel Kondisi Jaringan Setelah Implementasi**

| No | Aspek                      | Kondisi Sesudah Implementasi                                                                                           |
|----|----------------------------|------------------------------------------------------------------------------------------------------------------------|
| 1  | Sumber Internet            | Menggunakan koneksi internet berbasis <i>fiber</i> yang lebih stabil dan tidak terpengaruh sinyal maupun kondisi cuaca |
| 2  | Performa Jaringan          | Koneksi lebih stabil dengan penurunan <i>latency</i> dan minim <i>buffering</i> saat digunakan bersama                 |
| 3  | Manajemen <i>Bandwidth</i> | Menerapkan pembatasan <i>bandwidth</i> (3 Mbps & 50 Mbps) sehingga penggunaan lebih terkontrol                         |
| 4  | Keamanan Jaringan          | Pembatasan akses Internet sesuai kebijakan menggunakan <i>firewall</i> Mikrotik                                        |
| 5  | <i>Monitoring</i> Jaringan | Jaringan sudah dapat di <i>monitoring</i> , dan dapat diakses <i>monitoring</i> dari luar jaringan                     |

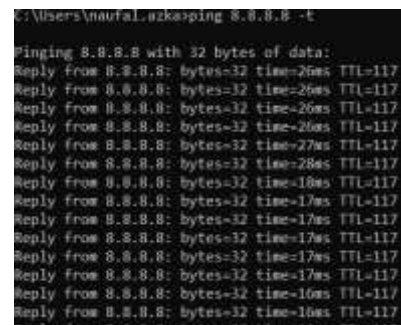
Untuk pengujian berikutnya, dilakukan akses *youtube* dan *speedtest*, selama pengujian berlangsung tidak ada terasa lag dan *speedtest* tidak ada *latency* maupun *jitter* yang tinggi. Pengetesan *ping* ke *DNS Google* juga lebih stabil.



**Gambar 44, Akses Youtube Setelah Implementasi**



**Gambar 45, Akses Speedtest Setelah Implementasi**



**Gambar 46, Pengetesan ping ke DNS Google Setelah Implementasi**

Berikutnya untuk *game online* yang dilakukan blokir pada mikrotik, sudah berhasil terblokir, untuk pengecekan nya di saat membuka *game*, aplikasi *game* hanya stak di *loading screen* nya, dan tidak dilanjutkan ke *lobby game* nya.



**Gambar 47, Blokir Game Mobile Legends**  
**Analisis Perbandingan Sebelum dan Setelah Implementasi**



**Gambar 48, Blokir Game PUBG**

Analisis perbandingan ini dilakukan untuk melihat perbedaan kondisi jaringan sebelum dan setelah implementasi, serta mengetahui peningkatan kualitas jaringan di Marqiz Imam Syafi'i dan Musholla Imam Syafi'I Condet.

Sebelum implementasi, jaringan masih memiliki kendala seperti koneksi yang belum stabil, belum adanya pengaturan *bandwidth*, dan belum tersedia sistem *monitoring* dan manajemen jaringan. Hal tersebut menyebabkan penggunaan jaringan kurang terkontrol,

Setelah implementasi, kondisi jaringan menjadi lebih stabil dan penggunaan *bandwidth* sudah dapat diatur per *subnet*, sehingga distribusi jaringan menjadi lebih merata. Selain itu, *monitoring* jaringan juga sudah dapat dilakukan secara jarak jauh, sehingga memudahkan pengelolaan.

**Tabel 2, Tabel Perbandingan Kondisi Jaringan Sebelum dan Setelah Implementasi**

| No | Parameter           | Sebelum Implementasi | Setelah Implementasi  |
|----|---------------------|----------------------|-----------------------|
| 1  | Koneksi Internet    | Tidak stabil         | Lebih stabil          |
| 2  | Manajemen Bandwidth | Belum ada            | Sudah diterapkan      |
| 3  | Akses Internet      | Tidak terkontrol     | Lebih terkontrol      |
| 4  | Performa Streaming  | Sering buffering     | Lebih lancar          |
| 5  | Monitoring          | Tidak tersedia       | Tersedia (jarak jauh) |

Berdasarkan Tabel 3, dapat dilihat bahwa implementasi yang dilakukan memberikan peningkatan terhadap kualitas jaringan. Hal ini terlihat dari koneksi yang menjadi lebih stabil, pengelolaan *bandwidth* yang lebih teratur, serta kemudahan dalam melakukan *monitoring* dan manajemen jaringan.

## KESIMPULAN

Berdasarkan hasil yang telah dilakukan pada Marqiz Imam Syafi'i dan Musholla Imam Syafi'i Condet, dapat disimpulkan bahwa implementasi jaringan berbasis Mikrotik mampu meningkatkan kestabilan koneksi internet sehingga aktivitas operasional dan live streaming berjalan lebih optimal, didukung oleh penerapan manajemen *bandwidth* yang membuat pembagian *bandwidth* lebih merata dan terkontrol, serta konfigurasi firewall yang membatasi akses sesuai kebijakan sehingga penggunaan internet menjadi lebih aman dan terarah, ditambah dengan sistem *monitoring* jarak jauh yang memudahkan administrator dalam pengawasan tanpa harus berada di lokasi; adapun untuk pengembangan ke depan disarankan agar dilakukan perawatan perangkat jaringan secara berkala guna menjaga kinerja tetap optimal, penggunaan internet diatur secara bijak oleh pengguna agar tidak mengganggu pengguna lain, pengelolaan jaringan terus ditingkatkan melalui evaluasi rutin terhadap kondisi dan kebutuhan, serta pengembangan sistem jaringan dilakukan secara bertahap menyesuaikan kebutuhan operasional.

## REFERENSI

- Alhaq, D. L., & Castrawijaya, C. (2025). Perkembangan Teknologi dan Pengembangan Sumber Daya Manusia Pada Lembaga Dakwah Majelis Ulama Indonesia (MUI). *Al Iman: Jurnal Keislaman Dan Kemasyarakatan*, 9(2), 877–900.
- AZ, I. B., Pt, S., Zahid Nugrah Arafah, S. H., Aldy Al Faisal, S., Very, J., Kom, S., & MM, M. (2025). *Perkembangan Teknologi Jaringan Nirkabel*. Fahmi Karya.
- Bilhanet.com. (2025). *Daftar Port Game Online untuk MikroTik Firewall*. Bilhanet.Com.
- Danuasmo, S., Nazuarsyah, N., & Ginting, R. B. (2023). Rancang bangun jaringan wireless LAN dan internet berbasis cloud pada Universitas Bina Bangsa Getsempena. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, 7(1), 15–24.
- Dewi, G. I. (2025). Analisis Strategi Peningkatan Mutu Pendidikan Islam Di Era Digital. *Majalah Ekonomi*, 31(1), 60–72.
- Fabiar, S. R. (2024). *Dakwah di era digital: Potret aktivitas dakwah Nawaning*. Penerbit Nem.
- Fajar Rayhan Putra Irawan, S. M., Aulia Rahman Anzari, S. M., Junisa Fitri, S., Muhammad Aliffarras Prasetyo, S., Jhon Veri, S., & MM, M. (2025). *Peran Telekomunikasi dan Jaringan dalam Inovasi Pelayanan Publik*. Fahmi Karya.
- Hafiz, A., & Kurnia, I. (2021). Mengembangkan jaringan wireless local area network (WLAN) dan hotspot pada AMIK Dian Cipta Cendikia (DCC) Pringsewu menggunakan router Mikrotik. *Jurnal Informatika Software dan Network (JISN)*, 2(1).
- Hasmiza, H. (2025). Model kurikulum pendidikan Islam di era digital: Mengoptimalkan teknologi untuk pembelajaran yang inovatif. *Research and Development Journal of Education*, 11(1), 164–177.
- Karyadi, J. (2025). Sinergi Teknologi, Spiritualitas, dan Humanitas dalam Membangun Budaya Organisasi Pendidikan Islam yang Adaptif. *Manajemen Pendidikan Islam Transformatif: Era Society 4.0 Dan Industri*, 5, 76.
- Kurniawan, D., & Rojabi, M. A. (2026). *Opera Mini: Revolusi Efisiensi Penjelajahan Web Hemat Data*. Afdan Rojabi Publisher.
- Lestari, N. (2024). Optimalisasi dakwah di era modern melalui media sosial. *Qawwam: The Leader's Writing*, 5(1), 35–42.
- Loho, A., & Ilham, R. (2025). *Analisis Infrastruktur Jaringan Komputer Menggunakan Analisis Swot Di Distrik Elelim Kabupaten YALIMO*. Fakultas Manajemen Pemerintahan.
- Purba, M. M., Amazihono, E., Panggabean, D., Sagala, T., Sinurat, N., & Hulu, A. (2025). Pengaruh Daerah Sulit Akses Jaringan Terhadap Efektivitas Pembelajaran Siswa. *Journal Education, Sociology and Law*, 1(1), 395–402.
- Rani, S. (2023). Transformasi komunikasi dakwah dalam era digital: Peluang dan tantangan dalam pendidikan Islam kontemporer. *AL-MIKRAJ Jurnal Studi Islam Dan Humaniora (E-ISSN 2745-4584)*, 4(1), 207–216.
- Sukmawati, D., Hamizar, A., & Tangke, D. M. (2024). Adopsi Teknologi Penggunaan Layanan Online-to-Offline (O2O) Masyarakat Wilayah Pesisir. *Journal of Business Application*, 3(2), 110–119.
- Wibowo, A. (2024). Teori Ekonomi Berbasis Big Data. *Penerbit Yayasan Prima Agus Teknik*, 1–253.