IMPLEMENTASI *DOMAIN NAME SYSTEM* (DNS) *FILTERING* MIKROTIK UNTUK PEMBATASAN AKSES MEDIA SOSIAL (STUDI KASUS: LABORATORIUM JARINGAN UNIVERSITAS DHYANA PURA)

Gustin Rikmartin Kroons, I Nyoman Bernadus, Putu Wida Gunawan
Informatika, Universitas Dhyana Pura
Jalan Raya Padang Luwih, Dalung, Kuta Utara, Badung, Bali, Indonesia
bernadus@undhirabali.ac.id

ABSTRAK

Internet dan jaringan komputer saat ini telah menjadi tulang punggung aktivitas akademik di lingkungan pendidikan, di mana ketersediaan akses yang stabil sangat krusial untuk mendukung kelancaran proses belajar mengajar. Namun, permasalahan sering terjadi pada manajemen *bandwidth* di Laboratorium Jaringan Universitas Dhyana Pura, yakni koneksi internet belum berjalan optimal dan sering mengalami gangguan berupa akses yang lambat terutama pada saat jam praktikum. Penyebab utama kendala tersebut adalah penggunaan internet yang tidak terkontrol untuk aktivitas luar akademik, seperti mengakses media sosial Instagram, TikTok, dan Facebook yang memicu pemborosan *bandwidth*. Oleh karena itu, penelitian ini bertujuan untuk merancang dan menerapkan *Domain Name System* (DNS) *Filtering* pada perangkat MikroTik sebagai solusi manajemen jaringan untuk membatasi akses ke media sosial tersebut. Penelitian ini dikembangkan menggunakan metode *Network Development Life Cycle* (NDLC) yang diadaptasi menjadi lima tahapan utama, yaitu analisis, desain, simulasi, implementasi, dan pemantauan (*monitoring*). Hasil pengujian menunjukkan bahwa metode ini efektif dalam memblokir akses pengguna ke media sosial yang ditargetkan. Selain itu, pemantauan trafik pasca-implementasi menunjukkan adanya penurunan penggunaan *bandwidth* yang sangat signifikan hingga kembali stabil, yang membuktikan bahwa penerapan DNS *Filtering* mampu mengoptimalkan ketersediaan internet untuk menunjang kegiatan akademik yang lebih produktif.

Kata kunci : *MikroTik, DNS, Internet, Bandwidth, Jaringan.*

1. PENDAHULUAN

Perkembangan teknologi internet dan jaringan komputer telah menjadi tulang punggung aktivitas akademik di berbagai lingkungan pendidikan, termasuk Universitas yang membutuhan koneksi internet yang stabil dan efisien adalah hal penting guna mendukung proses belajar mengajar [1].

Ketersediaan akses internet yang stabil dan berkualitas sangat diperlukan untuk mendukung proses belajar mengajar, pencarian referensi ilmiah, serta kegiatan akademik lainnya. Oleh karena itu, infrastruktur jaringan yang handal menjadi faktor penting dalam menunjang kelancaran dari aktivitas tersebut. Laboratorium jaringan Universitas Dhyana Pura sudah terkoneksi dengan jaringan internet, Masalah utama yang dihadapi pada saat praktikum adalah tingginya akses media sosial oleh mahasiswa yang mengakibatkan berkurangnya fokus belajar, menurunnya efektivitas praktikum, serta terganggunya kinerja jaringan dan konsumsi *bandwitdth* yang berlebihan. Kondisi ini dapat dirasakan pada saat jam praktikum, di mana terjadi penurunan kualitas koneksi internet seperti lambatnya akses dan tidak stabilnya koneksi internet. Permasalahan tersebut dibutuhkan akses kontrol dalam pembatasan akses khususnya media sosial sehingga pengelolaan sumber daya jaringan menjadi patokan dalam menjaga kualitas internet agar menjadi lebih stabil [2].

Penggunaan internet yang tidak terkontrol, menjadi salah satu faktor menurunnya kinerja layanan jaringan. Terutama saat mengakses media sosial seperti Instagram, TikTok, Facebook. Hal inilah yang menjadi tantangan dalam pembatasan akses. Meskipun media sosial, bermanfaat dalam hal berkomunikasi, tetapi juga memiliki dampak buruk seperti dalam lingkungan kampus yakni proses pembelajaran berupa gangguan konsentrasi belajar, yang dimana secara tidak langsung itu memengaruhi fokus proses pembelajaran dari mahasiswa [3]. Perihal penggunaan internet kini harus mendapat perhatian penting, demi terciptanya lingkungan akademik yang sehat. Mengatasi inti permasalahan, maka diperlukan sebuah opsi metode *Filtering* yang diharapkan mampu mengontrol dan membatasi akses dengan menggunakan perangkat MikroTik [4].

Salah satu solusi yang cukup efektif ialah dengan menerapkan *Domain Name System* (DNS) *Filtering* MikroTik. DNS *Filtering* ini bekerja dengan menyeleksi segala permintaan dari nama *domain* untuk dialihkan ataupun diblokir aksesnya sesuai daftar *blocklist*. Penerapan dari DNS *Filtering* diharapkan mampu mengoptimalkan *bandwidth*, agar penggunaan jaringan internet yang di konfigurasi menjadi stabil, efektif serta lebih terpusat [5].

Oleh karena itu, diperlukan solusi berupa implementasi DNS *Filtering* menggunakan Mikrotik. Dengan metode ini, penulis dapat membatasi akses ke *domain* tertentu khususnya media sosial, seperti Facebook, Instagram, dan TikTok. Hasil penelitian ini diharapkan jaringan internet lebih terkontrol, fokus pembelajaran praktikum meningkat, serta penggunaan

bandwidth lebih efisien di Laboratorium Jaringan Universitas Dhyana Pura.

2. TINJAUAN PUSTAKA

PenelItian tentang DNS *Filtering* telah dilakukan oleh Dadang Iskandar Mulyana dkk (2024) dengan penelitian yang berjudul "Optimasi Keamanan Jaringan Wi-Fi dari Situs Judi Online dan Pornografi dengan DNS *Filtering* dan Orangepi". Dalam penelitiannya menunjukkan bahwa dengan menggunakan DNS *Filtering* dan Orangepi dalam jaringan Wi-Fi terkhusus di balai warga RW 32 Bekasi mampu mengatasi akses situs yang tidak di inginkan dalam lingkungan masyarakat tujuannya untuk melindungi keamanan Wi-Fi atau jaringan yang di gunakan.

2.1. Jaringan Internet

Berdasarkan penelitian yang dilakukan oleh D. Maharani dkk (2021) menyimpulkan bahwa jaringan internet merupakan pertukaran data dan informasi yang tidak dibatasi oleh jarak dari antar perangkat, Internet menghubungkan berbagai perangkat, mulai dari komputer pribadi, *server*, hingga perangkat *Mobile.* Sebagai sebuah jaringan, internet berfungsi sebagai media komunikasi yang menyediakan berbagai layanan, mulai dari akses informasi, pengiriman data, dan layanan aplikasi [6].

2.2. Perangkat Jaringan

Menurut penelitian N. Heryana dkk (2021) Perangkat jaringan merupakan komponen fisik yang digunakan untuk menjalankan sistem pada jaringan komputer [7]. Adapun contoh perangkat jaringan yang penting pada penelitian penulis yaitu MikroTik.

2.3. MikroTik

Seperti yang dijelaskan oleh B. Cahya dkk (2023) MikroTik merupakan rangkaian perangkat jaringan yang terbagi menjadi MikroTik RouterBoard dan RouterOS. MikroTik RouterBoard adalah perangkat kerasnya, sedangkan sistem operasinya disebut RouterOS. Mikro Tik ini mendukung berbagai fitur manajemen jaringan seperti pengaturan *Internet Protocol* (IP), *Firewall*, *Domain Name System* (DNS), serta pengaturan *Routing* [8].

2.4. WinBox

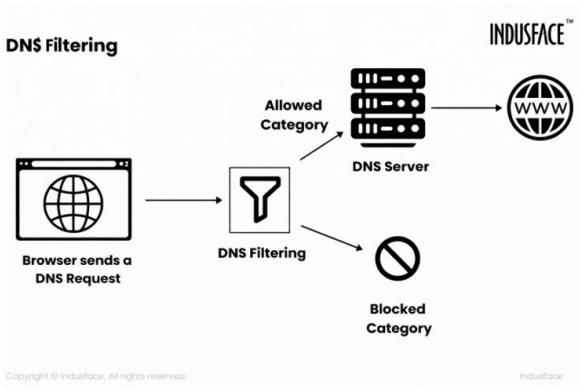
Dalam penelitian yang dilakukan oleh D. W. Ilahi dkk (2025) WinBox adalah aplikasi berbasis *Graphical User Interface* (GUI) yang dapat memudahkan konfigurasi dan manajemen perangkat [9]. Dalam penelitian ini, WinBox digunakan sebagai alat bantu untuk melakukan konfigurasi DNS *Filtering* pada MikroTik RouterOS, mulai dari pengaturan DNS *server*, pembuatan aturan pemblokiran, hingga proses *monitoring* hasil dari implementasi

2.5. *Domain Name System*

Penelitian yang dilakukan oleh Saputra Suhada et al.,(2024) menyimpulkan bahwa *Domain Name System* (DNS) adalah aplikasi *service* yang digunakan di internet seperti pada web browser unuk menerjemahkan sebuah nama *domain* dari IP *address*. Simpelnya DNS ini adalah penerjemah pengguna dengan bahasa komputer. Ketika mengakses media sosial Instagram, pengguna hanya perlu mengetik nama *domain* tanpa perlu menghafal dan menuliskan angka yang ada pada alamat IP media sosial Instagram [10] .

2.6. *Domain Name System Filtering*

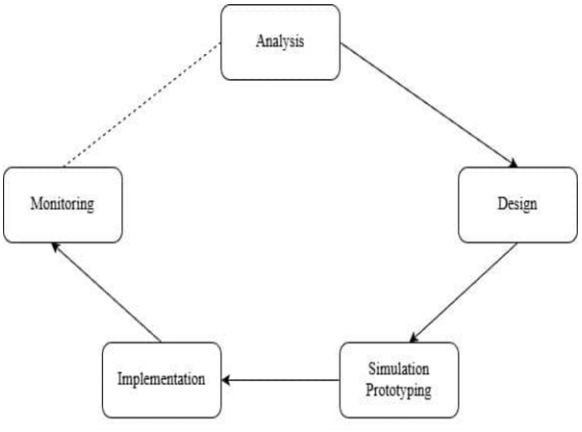
Penelitian yang dilakukan oleh I. Wahidaturrahmi dkk (2025) menyatakan bahwa *Domain Name System Filtering* adalah pemblokiran berdasarkan nama *domain*, misalnya jika ingin membatasi pengaksesan Facebook, otomatis pengguna yang akan mengaksesnya akan di batasi aksesnya ataupun dialihkan ke situs lain. DNS *Filtering* ini mencegah pengaksesan ke dalam situs yang sudah masuk daftar blokir atau ke situs yang tidak aman, serta DNS *Filtering* juga dapat melindungi dari berbagai ancaman serangan seperti *phising* dan *malware* [11].



Gambar 1. DNS *Filtering*

3. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah *Network Development Life Cycle* (NDLC), NDLC adalah sebuah model proses pengembangan tahapan pada jaringan komputer yang dilakukan secara bertahap [12]. NDLC mempunyai 6 tahapan pengembangan yaitu *Anaylsis*, *Design*, *Simulation Prototyping*, *Implementation*, *Monitoring*, serta *Management*. Pada penelitian penulis, tahapan NDLC diserhanakan menjadi 5 tahapan pengembangan yaitu *Anaylsis*, *Design*, *Simulation*, *Implementation*, dan *Monitoring*. Tujuan penyederhanaan ini agar tahapan metode NDLC sesuai dengan kebutuhan penelitian penulis. Berikut adalah gambar metode NDLC.



Gambar 2. NDLC

3.1. *Analysis*

Tahap analisis merupakan tahap awal yang bertujuan untuk mengidentifikasi *existing* (permasalahan saat ini) dan kebutuhan jaringan. Pada tahap ini dilakukan pengumpulan data terkait kondisi jaringan yang sedang berjalan, kebutuhan pengguna, serta permasalahan akses media sosial pada jaringan. Hasil dari tahap analisis digunakan sebagai dasar dalam perancangan *Domain Name System Filtering* menggunakan MikroTik.

3.2. *Design*

Design dilakukan untuk merancang solusi jaringan berdasarkan hasil analisis. Dari data yang sudah didapatkan sebelumnya, pada tahap ini akan membuat gambar rancangan topologi jaringan yang diharapkan dapat berjalan sesuai dengan kebutuhan dan tujuan penelitian.

3.3. *Simulation Prototyping*

Simulation prototyping, penulis menggunakan simulasi pemblokiran menggunakan router MikroTik dan fitur *Firewall* WinBox pada gedung A lantai 3 Laboratorium Jaringan Universitas Dhyana Pura.

3.4. *Implementation*

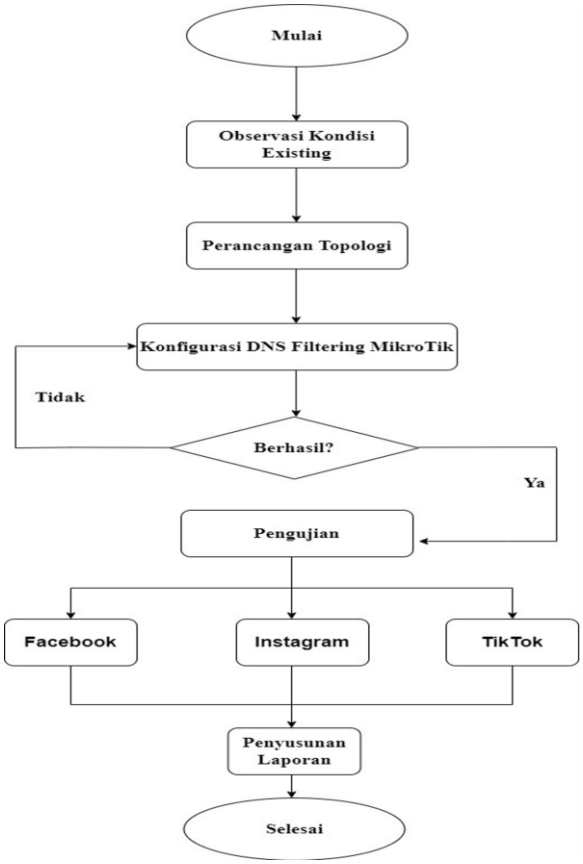
Tahap implementasi merupakan tahap penerapan nyata dari desain yang telah dibuat. Pada tahap ini dilakukan konfigurasi *Domain Name System Filtering* pada *router* MikroTik menggunakan WinBox. Implementasi dilakukan secara bertahap untuk memastikan DNS *Filtering* berjalan dengan baik dan sesuai dengan perencanaan.

3.5. *Monitoring*

Monitoring untuk memantau kinerja jaringan setelah diimplementasikan. Pada tahap ini dilakukan pengujian dan pengamatan terhadap efektivitas dari penerapan *Domain Name System* (DNS) *Filtering* MikoTik dalam membatasi akses ke media sosial. Monitoring bertujuan untuk memastikan penerapan DNS *Filtering* berhasil berjalan secara optimal sesuai dengan yang diharapkan.

3.6. Lokasi Penelitian

Lokasi penelitian ini berlokasi di Universitas Dhyana Pura Jalan Raya Padang Luwih Tegal Jaya, Dalung, Kuta Utara, Badung, Bali, Indonesia. Tempat pengujian Implementasi *Domain Name System Filtering* MikroTik berada pada gedung A lantai 3 di Laboratorium Jaringan. Waktu penelitian dilaksanakan penulis dari bulan Januari tahun 2026 sampai bulan Maret tahun 2026. Kerangka Penelitian dapat dilihat pada gambar dibawah ini.



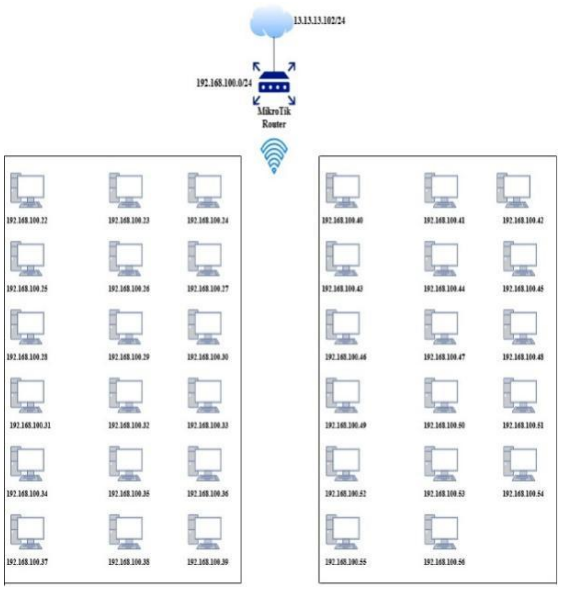
Gambar 3. Kerangka Penelitian

Dalam kerangka penelitian pada gambar 3. dipaparkan sebagai berikut:

a. Tahap observasi penulis lakukan dengan pengamatan secara langsung ke gedung A lantai 3 pada Laboratorium Jaringan Universitas Dhyana Pura.
b. Tahap perancangan topologi penulis lakukan dengan menentukan dan menyiapkan perangkat jaringan yang dibutuhkan dalam melakukan implementasi *Domain Name System* (DNS) *Filtering*.
c. Tahap ketiga adalah konfigurasi DNS *Filtering*
d. Tahap ke empat yaitu pengujian jaringan proses *monitoring* aktivitas dan efektivitas dari penerapan *Domain Name System* (DNS) *Filtering*. Tools yang digunakan penulis adalah WinBox.
e. Tahap terakhir adalah penyusunan laporan penelitian.

4. HASIL DAN PEMBAHASAN

4.1. Topologi Jaringan Laboratorium



Gambar 4. Topologi Jaringan

4.2. *Existing*

Berdasarkan observasi penulis, *existing* di Laboratorium Jaringan Universitas Dhyana Pura, saat ini terdapat total 36 unit komputer. Terdiri dari 1 komputer dosen pengajar dan 35 komputer *client* untuk mahasiswa, yang terhubung ke jaringan internet dimana semuanya dapat mengakses media sosial khususnya TikTok, Facebook, dan Instagram tanpa adanya pembatasan akses. Untuk mengetahui performa jaringan yang tersedia, penulis melakukan pengukuran total *bandwidth* dari *Internet Service Provider* (ISP) pada dua waktu dan proses pengujian yang berbeda.

Tabel 1. *Exiting*

Waktu	Pengujian	*Download* (Mbps)	*Upload* (Mbps)
09.00-13.30	Teori	108,46	140,10
14.00-15.30	Praktikum	128,92	138,72

Berdasarkan Tabel 1. penulis mendapat bahwa rata-rata *download* sebesar 118,69 Mbps. Jika diasumsikan seluruh 36 komputer yang digunakan secara bersamaan dibagi pada dua sesi saat teori dan praktikum, maka alokasi *bandwidth download* yang didapatkan setiap komputer adalah 3,29 Mbps.

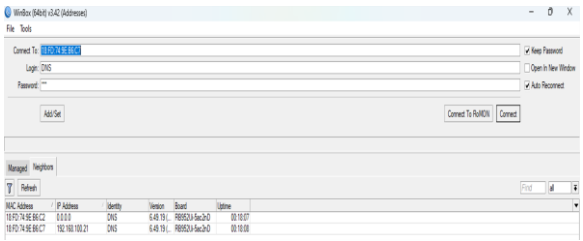
$$Bandwidth = \frac{118{,}69}{36} = 3.29\ Mbps \quad (1)$$

Selain pengukuran *download*, penulis juga melakukan analisis terhadap kapasitas *upload bandwidth*. Berdasarkan Tabel 4.1, rata-rata *upload* yang tersedia yaitu sebesar 139,41 Mbps. Dengan asumsi jumlah total pengguna yang sama 36 komputer, dengan dua waktu dan proses pengujian, maka didapatkan alokasi *bandwidth upload* per pengguna adalah 3,87 Mbps.

$$Bandwidth = \frac{139{,}41}{36} = 3.87\ Mbps \quad (2)$$

4.3. Implementasi *Domain Name System* (DNS) *Filtering* MikroTik

Penulis melakukan proses implementasi berdasarkan alur dan topologi yang sudah dibuat sebelumnya, dengan menggunakan WinBox. Dimulai dari penginputan IP *address*, sampai pada tahapan pengujian *Domain Name System Filtering*.

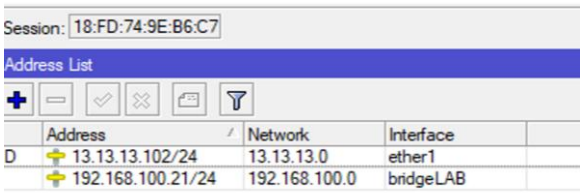


Gambar 5. Tampilan Utama WinBox

Penulis menggunakan WinBox versi 3.42 (64bit) pada gambar tersebut, terdapat perangkat MikroTik penulis dengan MAC *address* 18:FD:74:9E:B6:C7 dan IP *address* 192.168.100.21 yang menggunakan *login* DNS, Board RB952Ui-5ac2nD versi 6.49.19

4.4. Konfigurasi *Address List*

Penulis melakukan melakukan konfigurasi *address List* pada *router* MikroTik, dengan IP *Public* 13.13.13.102/24 dan network 13.13.13.0 yang dihubungkan ke *interface* ether1 yakni sumber internet (ISP), dan berikutnya IP *address* 192.168.100.21/24 dengan *network* 192.168.100.0 yang dihubungkan ke *interface* bridgeLAB. Penggunaan *interface* bridgeLAB penulis buat untuk menggambungkan jalur dari kabel dan nirkabel menjadi satu segmen jaringan, sehingga IP ini akan menjadi *gateway* (gerbang) dari semua lalu lintas data yang ada pada Laboratorium Jaringan. Konfigurasi ini dibuat agar memastikan semuanya dapat saling terkoneksi. *Address List* dapat dilihat pada gambar 6.

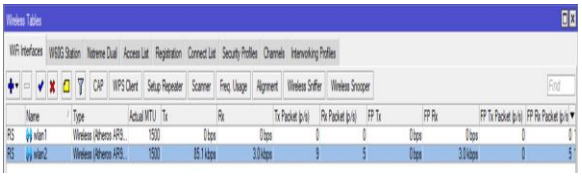


Gambar 6. *Address List*

4.5. Konfigurasi Wireless

Agar *router* dapat memancarkan sinyal Wi-Fi dan dikoneksikan oleh perangkat, penulis melakukan konfigurasi pada *interface* wlan1 dan wlan2. Langkah pertama adalah membuat *Security Profile* untuk

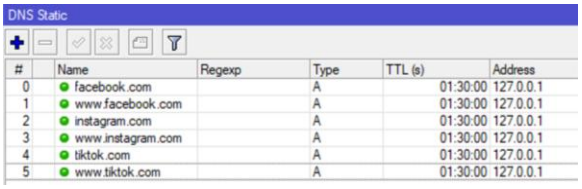
memberikan kata sandi pada Wi-Fi agar membatasi perangkat, sehingga cukup pengguna lab yang bisa terhubung. Selanjutnya, penulis mengaktifkan *interface* wlan1, wlan2 dan mengubah mode menjadi ap-bridge. Penulis memberi *Service Set Identifier* (SSID) atau nama Wi-Fi yang bernama DNS LAB JAR. Selain itu, *interface* wlan1 dan wlan2 ini juga dimasukkan ke dalam bridgeLAB agar tergabung dalam satu segmen jaringan dengan ethernet, sehingga aturan pembatasan akses yang diterapkan nanti dapat berlaku untuk semua jalur. *Wireless Tables* dapat dilihat pada gambar 7.



Gambar 7. *Wireless Tables*

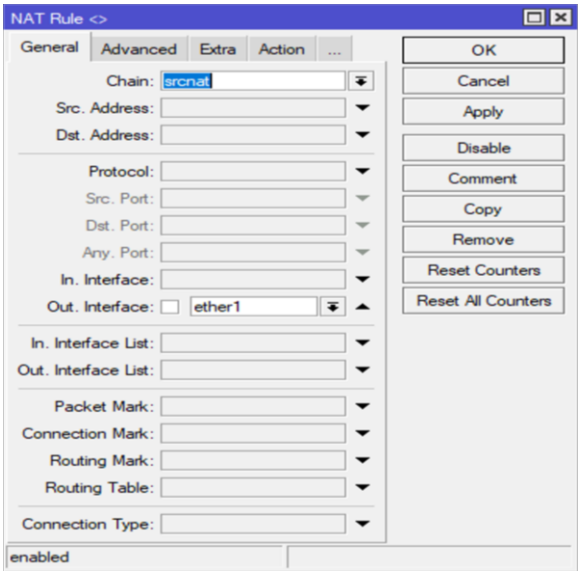
4.6. Konfigurasi DNS *Static*

Penulis memasukan daftar nama *domain* yang akan di blokir ke dalam *Static* DNS dan mengarahkan ke IP *Loopback* 127.0.0.1 dengan waktu 1 jam 30 menit per perangkat untuk bertanya kembali, tujuan dari konfigurasi ini agar nama domain pada daftar blokir tidak dapat diakses oleh pengguna yang terhubung ke jaringan yang telah penulis buat, dapat dilihat pada gambar 8.



Gambar 8. DNS *Static*

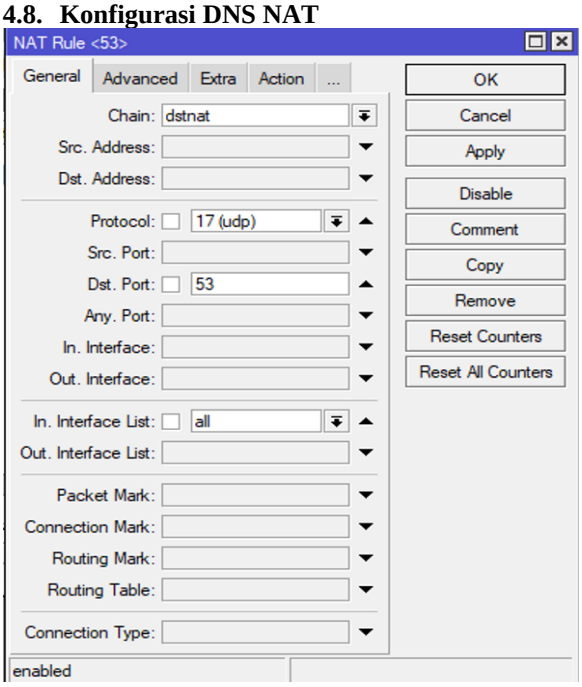
4.7. Konfigurasi *Network Address Translation*



Gambar 9. *Network Address Translation*

Setelah konfigurasi DNS selesai, langkah selanjutnya adalah penulis mengaktifkan *Network Address Translation* (NAT) pada menu *Firewall.* Konfigurasi ini sangat penting karena alamat IP lokal (192.168.100.0/24) yang digunakan pada jaringan laboratorium ini merupakan IP *Private* yang tidak dapat terhubung ke internet secara langsung. Penulis menambahkan NAT Rule dengan chain srcnat dan action masquerade pada *out interface* ether1. Konfigurasi ini bertujuan untuk menyembunyikan IP *address* klien dan menggantinya dengan IP *public router* saat mengakses internet, sehingga seluruh komputer di laboratorium dapat berselancar di internet menggunakan satu jalur keluar yang sama.

4.8. Konfigurasi DNS NAT



Gambar 10. *Network Address Translation*

Selanjutnya adalah melakukan konfigurasi DNS NAT pada menu *Firewall*. Penulis membuat chain dstnat dan *protocol* 17 dengan dst port 53 *interface list all*.*Protocol* 17 adalah kode standar dari *User Datagram Protocol* (UDP), UDP ini tujuannya mengirimkan paket data dengan cepat dan efisien untuk permintaan singkat dibanding *Transmission Control Protocol* (TCP). Dst Port 53 adalah port standar global yang khusus buat layanan DNS. Konfigurasi ini bertujuan untuk memaksa (*redirect*) semua permintaan pengguna agar masuk terhubung dengan aturan *router* MikroTik. *Router* MikroTik ini dapat mengaktifkan fitur *Allow Remote Requests* untuk sebagai DNS *Cache.* Hasilnya jika satu komputer mengakses sebuah *domain* media sosial, maka *router* akan menyimpan alamat IP dari media sosial tersebut, jadi Ketika komputer lain yang ada di lab mengakses ke *domain* yang sama, maka *router* langsung menjawab tanpa perlu bertanya lagi ke internet, sehingga proses *loading* lebih cepat dan membuat *bandwidth* menjadi efisien.

4.9. Konfigurasi DHCP *Server*

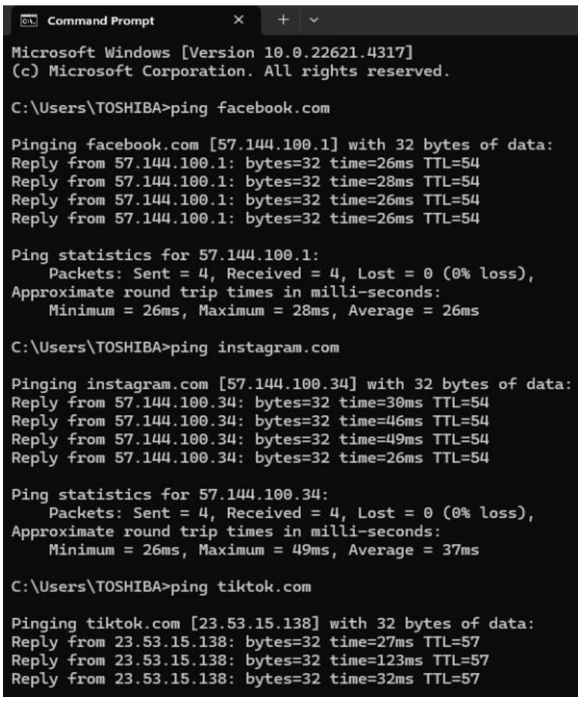
Penulis melakukan konfigurasi *Dynamic Host Configuration Protocol* (DHCP) *Server* pada *interface* bridgeLAB, untuk mempermudah manajemen pengalamatan IP pada komputer mahasiswa. Dengan adanya DHCP *Server*, setiap perangkat yang erhubung ke jaringan melalui kabel ataupun Wi-Fi akan mendapatkan konfigurasi jaringan secara otomatis, meliputi IP *address*, *Netmask*, *Gateway* (192.168.100.21), dan DNS *Server*. Hal ini membuat waktu menjadi jauh lebih efisien karena tidak perlu lagi untuk melakukan konfigurasi IP secara manual (*static*) satu per satu dari setiap perangkat yang ada.

4.10. Hasil Pengujian

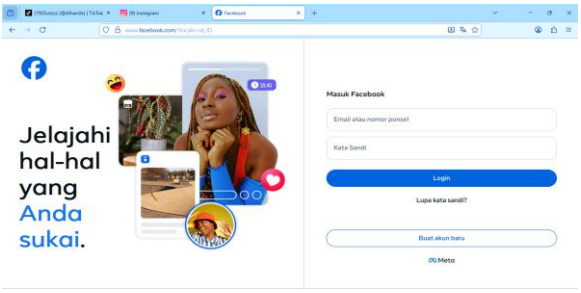
Setelah seluruh konfigurasi yang sudah berjalan, maka berikutnya penulis melakukan pengujian untuk memverifikasi keberhasilan konfigurasi yang dibuat, untuk membatasi akses terhadap *domain* media sosial dan efisiensi dari penggunaan *bandwidth*. Pengujian ini penulis bagi menjadi dua tahap penerapan, yang pertama sebelum penerapan DNS *Filtering* MikroTik dan yang kedua yaitu sesudah penerapan DNS *Filtering* MikroTik.

4.11. Sebelum Penerapan DNS *Filtering* MikroTik

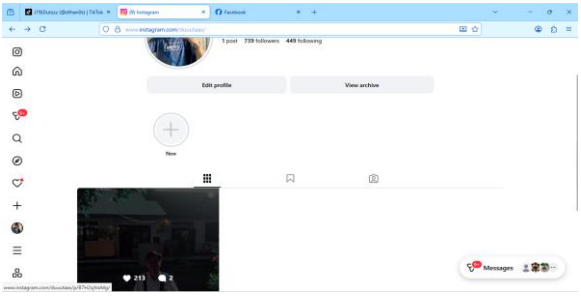
Penulis melakukan pengujian dengan ping menggunakan command prompt dan mengakses ke *domain* media sosial Facebook, Instagram dan TikTok menggunakan browser Mozilla Firefox yang ada dalam komputer di Laboratorium Jaringan. Pada saat ini media sosial masih dapat diakses, karena daftar blokir masih belum di terapkan oleh penulis yang dapat dilihat pada gambar dibawah ini.



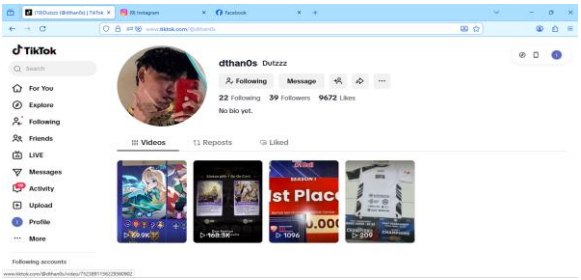
Gambar 11. Command Prompt Ping Media Sosial *Before*



Gambar 12. Media Sosial Facebook



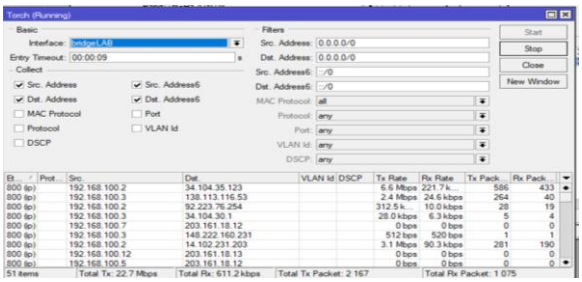
Gambar 13. Media Sosial Instagram



Gambar 14. Media Sosial TikTok

4.12. *Bandwidth* Sebelum Penerapan DNS *Filtering* MikroTik

Setelah pengujian berhasil mengakses ke media sosial Facebook, Instagram, serta TikTok. Selanjutnya penulis melakukan pemantauan trafik, menggunakan *Torch* WinBox yang ada pada *interface* bridgeLAB. Disini tercatat aktivitas Total Tx 22,7 Mbps, dan total Rx 611,2 Kbps, ini terbukti valid mengindikasikan penggunaan *bandwidth* yang cukup besar untuk kegiatan di luar akademik, dapat dilihat pada gambar 15.

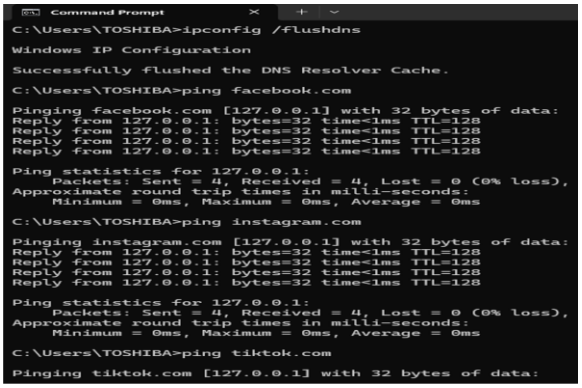


Gambar 15. *Torch Bandwidth Before*

4.13. Sesudah Penerapan DNS *Filtering* MikroTik

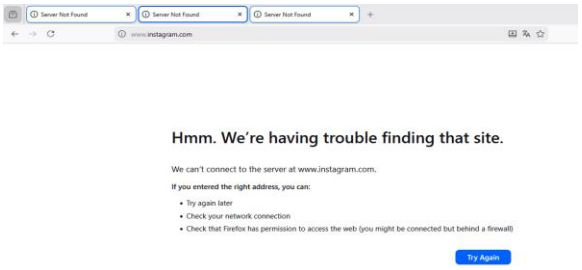
Pada tahap ini, penulis mengaktifkan DNS *Static* untuk memastikan pengujian berjalan dengan valid, penulis juga melakukan *Flush Cache*. Berdasarkan

pengujian menggunakan ping dari Command Prompt, terlihat bahwa *domain* dari Facebook, Instagram, dan TikTok merespon dengan alamat IP 127.0.0.1. Hal ini membuktikan bahwa akses ke alamat aslinya telah dibatasi dan dialihkan ke alamat *localhost*.



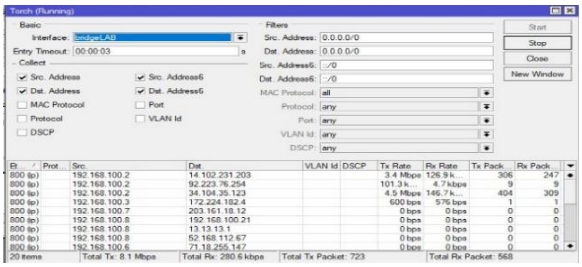
Gambar 16. Command Prompt Ping Media Sosial *After*

Berikutnya penulis melakukan pengujian kembali mengunakan browser pada komputer di Laboratorium Jaringan, yang dimana menampilkan akses ke media sosial Instagram menjadi *Server Not Found* atau tidak dapat diakses, serta menunjukan pesan *error*. Pesan *error* ini terjadi karena *Domain Name System* (DNS) *Filtering* telah berhasil diterapkan, sehingga browser tidak mendapatkan alamat IP publik yang valid dari nama domain media sosial tersebut. *Error* tersebut membuktikan bahwa browser telah di batasi dan alamat IP telah dialihkan ke alamat *loopback* 127.0.0.1 oleh *router* MikroTik, seperti yang ada pada gambar 17.



Gambar 17. Media Sosial Sesudah Penerapan DNS *Filtering*

Hasil ini juga diperkuat dengan pengujian monitoring trafik data pemantauan lalu lintas jaringan. Penulis melakukan pemantauan trafik, menggunakan *Torch* WinBox pada *interface* bridgeLAB untuk melihat aktivitas penggunaan *bandwidth*, terlihat perbedaan Tx *Rate* dan Rx *Rate* yang kini menjadi turun secara signifikan dari sebelum penerapannya. Hal ini menunjukkan bahwa tidak ada lagi konsumsi *bandwidth* yang besar, sehingga membuat *bandwidth* menjadi lebih stabil dan efisien untuk digunakan, karena aliran data yang sering dilakukan untuk *streaming* pada media sosial Instagram, Facebook dan TikTok telah berhasil diblokir aksesnya. Serta terjadi penurunan pemakaian *bandwitdth* sebesar 8.1 Mbps. Bisa dilihat pada gambar 18.



Gambar 18. *Torch Bandwidth After*

5. KESIMPULAN DAN SARAN

Berdasarkan hasil implementasi dan pengujian yang telah dibahas pada bab-bab sebelumnya, penulis dapat menarik beberapa kesimpulan sebagai berikut:
Implementasi *Domain Name System Filterng* MikroTik telah berhasil dikonfigurasi di Laboratorium Jaringan Universitas Dhyana Pura. Penerapannya telah terbukti efektif untuk memblokir akses dari media sosial TikTok, Instagram, dan Facebook tanpa membatasi akses terhadap *domain* dari web pembelajaran, seperti SiPanDU. Pengujian ini menunjukkan bahwa media sosial yang sudah dibatasi tidak dapat lagi diakses oleh pengguna dan hanya memunculkan pesan *error*. Implementasi *Domain Name System Filtering* MikroTik ini berdampak positif terhadap efisiensi *bandwidth* di Laboratorium Jaringan Universitas Dhyana Pura. Terbukti dari hasil *monitoring Torch*, terjadi penurunan trafik dari sebelum pembatasan akses terhadap media sosial TikTok, Instagram, dan Facebook yang signifikan. Awalnya dari 22,7 Mbps menjadi jauh lebih efisien setelah pembatasan akses media sosial dibuat. Hal ini menjamin ketersediaan *bandwidth* yang cukup bagi pengguna di Laboratorium Jaringan untuk dipakai dalam kegiatan akademik.

Penelitian ini masih memiliki ruang untuk pengembangan lebih lanjut. Oleh karena itu, penulis memberikan beberapa saran sebagai berikut:
Penerapan *Scheduler*: Untuk pengembangan selanjutnya, sistem pemblokiran dapat dikombinasikan dengan fitur *Scheduler* dan *Scripting* agar pemblokiran hanya aktif pada jam perkuliahan, dan terbuka otomatis saat jam istirahat.

Penggunaan *Layer* 7 *Protocol*: Mengingat aplikasi media sosial terus berkembang, disarankan untuk mengkombinasikan metode DNS *Static* dengan *Layer* 7 *Protocol* atau *Firewall filter* untuk menangani aplikasi *mobile* yang mungkin menggunakan *Hardcoded* IP tidak hanya melalui DNS.

DAFTAR PUSTAKA

[1] N. Muhammad Wildan Putra Pratama, F. Fatchurrohman, and I. Budi Susanto, "Optimalisasi Jaringan Internet Dengan Menggunakaan Simple Queue Dan Firewall Mikrotik Di Sekolah Menengah Pertama Negeri

Kota Malang," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 8, no. 6, pp. 12828–12835, 2024, doi: 10.36040/jati.v8i6.12130.

[2] R. A. Paskal, "Tinjauan Literatur: Implementasi Manajemen Bandwidth," *Innov. J. Soc. Sci. Res.*, vol. 4, no. 4, pp. 8075–8090, 2024, [Online]. Available: https://j-innovative.org/index.php/Innovative/article/view/9670

[3] A. Ardiyanti, M. T. Rhamadani, R. A. Putri, S. Widya, and J. Tarigan, "Pengaruh Media Sosial Terhadap Konsentrasi Dan Fokus Belajar Mahasiswa / I Unimed Fakultas FBS," *BENEFIT J. Busines, Econ. Financ.*, vol. 3, no. 1, pp. 69–76, 2025, [Online]. Available: https://doi.org/10.70437/benefit.v3i1.1057

[4] H. A. Al Kautsar and R. Sastra, "Implementasi Firewall Mikrotik dalam Pembatasan Akses Situs Terlarang di RT/RW Net," *Comput. Sci.*, vol. 5, no. 2, pp. 123–132, 2025, doi: 10.31294/coscience.v5i2.8897.

[5] D. I. Mulyana, F. Ardiyansyah, N. Hidayat, and A. Zulfikar, "Optimasi Keamanan Jaringan Wifi dari Situs Judi Online dan Pornografi dengan DNS Filtering dan Orangepi," *MALCOM Indones. J. Mach. Learn. Comput. Sci.*, vol. 4, no. 2, pp. 647–655, 2024, doi: 10.57152/malcom.v4i2.1274.

[6] D. Maharani, F. Helmiah, and N. Rahmadani, "Penyuluhan Manfaat Menggunakan Internet dan Website Pada Masa Pandemi Covid-19," *Abdiformatika J. Pengabdi. Masy. Inform.*, vol. 1, no. 1, pp. 1–7, 2021, doi: 10.25008/abdiformatika.v1i1.130.

[7] N. Heryana et al, *PENGENALAN DASAR JARINGAN KOMPUTER*, vol. 32, no. 3. 2021.

[8] B. Cahya, F. Rizki, A. Sutiyo, Y. El Saputra, and M. Elfarizi, "Implementasi Firewall Pada Mikrotik Untuk Keamanan Jaringan," *J. JOCOTIS-Journal Sci. Inform. Robot. E*, vol. 1, no. 2, pp. 63–80, 2023, [Online]. Available: https://jurnal.ittc.web.id/index.php/jct/

[9] D. W. Ilahi and A. Samad, "Configurasi Setting Hotspot Dan Pppoe Dengan," vol. 2, no. 3, pp. 195–207, 2025.

[10] Saputra Suhada, Fadly Ariadi, and Anggreita Tiara Putri, "Pengenalan Domain Name Server Pada Siswa-Siswi Smk Puspita Bangsa," *Prax. J. Pengabdi. Kpd. Masy.*, vol. 4, no. 1, pp. 29–34, 2024, [Online]. Available: www.namaanda.com',

[11] I. Wahidaturrahmi and D. Priyanto, "Desain dan Implementasi CI/CD untuk Mengotomasi Sistem Pemblokiran Situs Judi Online Berbasis DNS Filtering," *Semin. Nas. Corisindo*, no. September 2025, pp. 450–456, 2025.

[12] F. Hari Prasetyo, E. Infitharina, and M. Febriyansyah, "Penerapan Metode Network Development Life Cycle (NDLC) dalam Pengembangan Jaringan Komputer," *JUNI 2025 J. Informatics Commun. Technol.*, vol. 7, no. 1, pp. 80–087, 2025.