IMPLEMENTASI DHCP SERVER DAN FIREWALL PADA ROUTER MIKROTIK UNTUK MENGELOLA JARINGAN LINGKUNGAN KOMINFO

Implementation of DHCP Server and Firewall on Mikrotik Router to Manage the Kominfo Environment Network

Yoga Tri Pramana, Raphael Bianco Huwae, Dwi Ratnasari, Andy Hidayat Jatmika
Dept Informatics Engineering, Mataram University
Jl. Majapahit 62, Mataram, Lombok NTB, INDONESIA
Email: luckydog744@gmail.com, raphaelbianco@unram.ac.id, dwi.ratnasari@unram.ac.id, andy@staff.unram.ac.id

Abstrak

Mikrotik merupakan salah satu perangkat jaringan yang banyak digunakan untuk mengelola dan mengoptimalkan konektivitas dalam berbagai skala jaringan. Artikel ini menyajikan panduan praktis untuk pengelolaan jaringan menggunakan Mikrotik, dengan fokus pada pengenalan perangkat, konfigurasi dasar, implementasi DHCP server, serta pengaturan firewall (filter). Tujuan dari makalah ini adalah untuk memberikan wawasan mendalam mengenai langkah-langkah penting dalam konfigurasi Mikrotik, yang dapat membantu administrator jaringan dalam mengoptimalkan performa dan keamanan jaringan. Melalui implementasi DHCP server memungkinkan manajemen jaringan yang lebih efisien, memungkinkan alokasi alamat IP secara otomatis, yang mengurangi kemungkinan konflik IP, dan mempermudah pengaturan perangkat yang terhubung dan mengoptimalkan penggunaan sumber daya jaringan. Selain itu, firewall memainkan peran penting dalam menjaga keamanan dan integritas data dengan menerapkan kebijakan akses yang ketat, menyaring lalu lintas berbahaya, dan mencegah serangan dari pihak yang tidak berwenang. Untuk memastikan pemahaman yang lebih mendalam tentang optimasi jaringan menggunakan Mikrotik, pelatihan teknis, simulasi konfigurasi, dan pendampingan langsung digunakan. dan diharapkan dapat diperoleh sebuah peningkatan efisiensi dalam pengelolaan jaringan serta peningkatan keamanan yang signifikan. Kesimpulan dari makalah ini menegaskan pentingnya pemahaman mendalam terhadap konfigurasi Mikrotik untuk menciptakan jaringan yang optimal dan aman.

***Kata Kunci**: Mikrotik, Konfigurasi Dasar, DHCP Server, Firewall*

1. PENDAHULUAN

Dalam era digital saat ini, kebutuhan akan pengelolaan jaringan yang efektif dan efisien semakin penting, khususnya bagi instansi pemerintah seperti Dinas Komunikasi Informatika dan Statistik Prov NTB. Pengelolaan jaringan yang baik memastikan akses internet yang stabil, aman, dan teratur bagi para pengguna. Salah satu perangkat yang sering digunakan dalam pengaturan jaringan adalah Mikrotik, yang dikenal karena fleksibilitas dan kemampuannya dalam menangani berbagai kebutuhan jaringan, mulai dari konfigurasi dasar hingga implementasi fitur-fitur keamanan seperti *firewall*.

Tanpa Mikrotik membuat manajemen jaringan lebih sulit dan rentan terhadap berbagai masalah. Salah satu masalah utama adalah masalah manajemen alamat IP. Tanpa fitur DHCP Server, administrator harus mengatur alamat IP secara manual, yang berpotensi menyebabkan konflik dan kesalahan konfigurasi. Tanpa firewall, keamanan jaringan juga berkurang karena serangan seperti malware, DDoS, dan akses tidak sah meningkat. Selain itu, tanpa routing yang baik, paket data tidak dapat dikirim dengan baik, menyebabkan latensi tinggi dan koneksi yang lambat, yang mengganggu stabilitas jaringan.

Sehingga penggunaan Mikrotik dalam lingkungan Kominfo memiliki peran vital, mengingat besarnya kebutuhan akan pengelolaan jaringan yang handal di tengah arus data yang terus meningkat. Beberapa fitur yang paling sering dimanfaatkan adalah konfigurasi dasar untuk pengaturan *IP*, implementasi *DHCP server* untuk distribusi alamat *IP* secara otomatis, serta pengaturan *firewall* guna melindungi jaringan dari potensi ancaman keamanan. Semua fitur ini perlu dikelola dengan baik agar infrastruktur jaringan dapat berfungsi optimal dan aman.

Jika sebuah organisasi seperti Kominfo tidak memiliki pengelolaan jaringan yang baik, maka beberapa masalah besar akan muncul. Misalnya, jaringan yang tidak dikelola dengan baik bisa mengalami penurunan kinerja, yang berakibat pada lambatnya akses internet. Ini bisa mengganggu operasional harian, seperti komunikasi antara pegawai, akses ke data penting, hingga proses pelayanan publik yang harus dilakukan secara cepat dan tepat waktu.

Sebagai contoh kasus yang pernah terjadi, dalam situasi di mana tidak ada pembatasan atau manajemen *bandwidth*, pegawai mungkin secara tidak sengaja menggunakan *bandwidth* yang besar untuk keperluan yang tidak terkait dengan pekerjaan, seperti *streaming* video atau unduhan *file* berukuran besar. Akibatnya, aplikasi atau layanan penting yang seharusnya mendapat prioritas dalam penggunaan *bandwidth* justru tidak berjalan optimal. juga menemukan bahwa tanpa adanya manajemen *bandwidth* yang baik, tingkat produktivitas pegawai menurun karena sering terganggu oleh jaringan yang lambat. Mikrotik dengan fitur *QoS*-nya memungkinkan administrator mengalokasikan *bandwidth* sesuai kebutuhan sehingga setiap layanan mendapatkan prioritas yang tepat [1].

Sebagai ilustrasi, sebuah lembaga yaitu Dinas Komunikasi Informatika dan Statistic dipemerintah Indonesia pernah menghadapi masalah besar dalam hal manajemen jaringan sebelum menggunakan Mikrotik. Lembaga tersebut mengalami berbagai serangan siber dan kinerja jaringan yang sangat lambat, terutama saat jam kerja. Setelah beralih ke Mikrotik, mereka mengimplementasikan *firewall* yang kuat, pengaturan *DHCP* yang dinamis, dan *QoS* untuk manajemen *bandwidth*. Hasilnya, dalam kurun waktu enam bulan, mereka mencatatkan peningkatan efisiensi jaringan hingga 30%, dengan serangan siber yang berhasil dicegah meningkat hingga 40% [2]. Implementasi MikroTik di lembaga tersebut tidak hanya meningkatkan performa jaringan tetapi juga menurunkan biaya operasional mereka dalam jangka panjang karena perangkat ini lebih hemat biaya dibandingkan dengan solusi jaringan lainnya.

Laporan ini berusaha untuk menjembatani kesenjangan yang ada dalam literatur saat ini dengan menyediakan panduan yang komprehensif dan praktis untuk pengelolaan jaringan menggunakan Mikrotik. Berdasarkan hal yang melatar belakangi sebelumnya, terlihat bahwa Mikrotik merupakan solusi yang kuat namun memerlukan pemahaman yang mendalam untuk diimplementasikan secara efektif. Artikel ini akan memberikan panduan yang disesuaikan dengan kebutuhan praktisi jaringan yang mungkin tidak memiliki latar belakang teknis yang mendalam, namun tetap ingin mengoptimalkan penggunaan Mikrotik untuk mengelola dan mengamankan jaringan mereka. Dengan demikian, laporan ini tidak hanya menambah literatur yang ada dengan panduan praktis, tetapi juga memberikan kontribusi signifikan dalam mempermudah adopsi teknologi Mikrotik di berbagai lingkungan jaringan.

2. TINJAUAN PUSTAKA

Penggunaan perangkat jaringan seperti Mikrotik untuk pengelolaan dan pengamanan jaringan telah menjadi topik penting dalam beberapa tahun terakhir, seiring dengan meningkatnya kebutuhan akan jaringan yang efisien dan aman. Berbagai penelitian dan publikasi telah membahas metode dan hasil yang berkaitan dengan implementasi Mikrotik dalam konteks ini. Tinjauan pustaka ini akan menguraikan beberapa pustaka terbaru yang relevan dengan topik artikel ini, serta memberikan ulasan kritis mengenai metode dan hasil yang telah dicapai.

2.1. Penerapan Mikrotik dalam Pengelolaan Jaringan

Beberapa studi terbaru menunjukkan bahwa Mikrotik dapat memberikan solusi yang efektif dalam pengelolaan jaringan, terutama untuk organisasi kecil hingga menengah, Mikrotik *RouterOS* dapat digunakan untuk membangun infrastruktur jaringan yang efisien dengan biaya yang relatif rendah dibandingkan dengan perangkat lain.[3] [4] Studi ini menunjukkan bahwa konfigurasi dasar Mikrotik, termasuk pengaturan *IP* dan *routing*, dapat diimplementasikan dengan cepat dan mudah, yang sangat bermanfaat bagi organisasi dengan sumber daya teknis yang terbatas.

Namun, terdapat hasil studi yang mencatat beberapa tantangan, terutama terkait dengan kurva belajar yang curam untuk pengguna yang baru mengenal Mikrotik. Oleh karena itu, laporan ini bertujuan untuk mengatasi tantangan tersebut dengan menyediakan panduan yang mudah diikuti, sehingga dapat memperluas manfaat Mikrotik ke pembaca yang lebih luas [5].

Dalam Praktik Kerja Lapangan masyarakat telah menyelidiki penggunaan Mikrotik dalam skala organisasi selain penelitian akademis. Pemahaman teknis tentang konfigurasi jaringan berbasis Mikrotik telah ditingkatkan melalui pelatihan berbasis praktik lapangan. Ini terutama berlaku untuk tenaga IT di lembaga pendidikan dan pemerintahan. Hasil kegiatan menunjukkan bahwa peserta memiliki keterampilan yang lebih baik dalam mengelola jaringan berbasis Mikrotik, yang berdampak pada efisiensi operasional dan keamanan jaringan mereka. Namun, hingga saat ini, sangat sedikit penelitian ilmiah yang membahas secara khusus penggunaan Mikrotik dalam Praktik Kerja Lapangan.

2.2. Implementasi *DHCP Server* pada Mikrotik

DHCP server merupakan komponen penting dalam pengelolaan jaringan, dan penggunaan Mikrotik sebagai *DHCP server* telah dibahas dalam beberapa studi terbaru. menunjukkan bahwa implementasi *DHCP server* pada Mikrotik dapat meningkatkan efisiensi distribusi alamat *IP* dalam jaringan dengan banyak perangkat.[6] [7] Dalam

studi mereka, Mikrotik terbukti mampu menangani distribusi *IP* dengan tingkat kesalahan yang sangat rendah, bahkan dalam lingkungan jaringan yang kompleks.

Penelitian lain mendukung relevansi topik ini dengan menjelaskan secara mendalam tentang implementasi *DHCP server* pada MikroTik. Meskipun studi-studi sebelumnya menunjukkan hasil yang positif, masih terdapat ruang untuk penelitian lebih lanjut terkait optimasi pengaturan *DHCP* pada Mikrotik, khususnya dalam skenario yang melibatkan *subnet* beragam dan perubahan topologi jaringan secara dinamis. Optimalisasi ini penting untuk meningkatkan efisiensi pengelolaan *IP address* [8] di mana pengaturan *DHCP* pada MikroTik membantu perusahaan mengelola distribusi *IP* secara optimal. Selain itu, studi lain menekankan pentingnya implementasi *DHCP server* berbasis Mikrotik di sekolah menengah atas untuk memastikan distribusi *IP* yang teratur [9]. Penelitian lainnya juga menunjukkan bahwa optimasi pengelolaan *DHCP* pada Mikrotik router mampu mengatasi masalah konflik *IP* yang sering terjadi dalam jaringan yang tidak terkelola dengan baik [10].

Dalam Praktik Kerja Lapangan, beberapa pelatihan telah dilakukan untuk meningkatkan pemahaman peserta tentang penerapan DHCP Server pada Mikrotik. Pelatihan yang ditujukan untuk tenaga IT di lembaga pemerintah dan institusi pendidikan telah membantu mengurangi kesalahan konfigurasi IP Address dan meningkatkan keandalan jaringan di tempat kerja mereka. Untuk mengetahui seberapa efektif praktik ini, perlu dilakukan penelitian lebih lanjut.

2.3. Pengaturan *Firewall* (Filter) dalam Keamanan Jaringan

Keamanan jaringan adalah salah satu aspek paling krusial dalam pengelolaan jaringan modern, di mana firewall berperan sebagai garis pertahanan utama dalam melindungi sistem dari berbagai ancaman siber. Mikrotik, dengan fitur *firewall* yang kuat, telah terbukti efektif dalam memblokir berbagai jenis serangan siber, termasuk *DDoS* (*Distributed Denial of Service*) dan *malware* [11]. menemukan bahwa konfigurasi *firewall* Mikrotik yang tepat mampu secara signifikan mencegah serangan terhadap jaringan internal serta melindungi data sensitif dari ancaman eksternal.

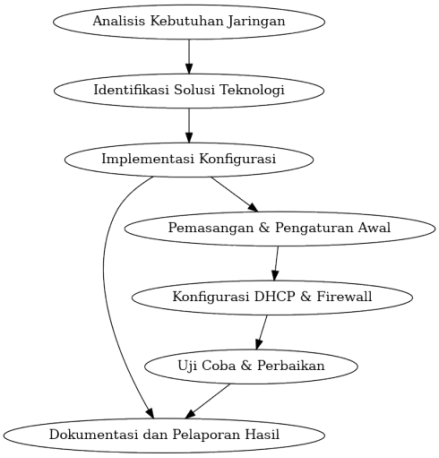
Selain itu, penelitian lain menunjukkan bahwa Mikrotik dapat dioptimalkan untuk melindungi jaringan internal dengan merancang aturan *firewall* yang membatasi akses berdasarkan *IP*, protokol, dan *port* tertentu, sehingga risiko kebocoran data dapat diminimalisasi [12]. ini juga diperkuat dengan catatam bahwa konfigurasi *firewall* Mikrotik dapat mencegah akses yang tidak diinginkan ke jaringan publik, menjaga keamanan sistem dari pengguna yang tidak sah [13].

Namun, penting untuk diingat bahwa efektivitas *firewall* tidak hanya bergantung pada konfigurasi awalnya menggarisbawahi pentingnya pemeliharaan rutin serta pembaruan konfigurasi *firewall* untuk menghadapi ancaman baru yang terus berkembang [14]. Studi lainnya menunjukkan bahwa penggunaan *firewall* Mikrotik di perusahaan dapat meningkatkan keamanan jaringan secara signifikan, khususnya dalam menangani ancaman-ancaman yang semakin kompleks di era digital. Dengan pendekatan yang komprehensif, Mikrotik mampu memberikan perlindungan jaringan yang handal dan dapat diandalkan jika dikonfigurasi dan dikelola secara berkelanjutan [15].

Dalam Praktik Kerja Lapangan, untuk meningkatkan kesadaran dan keterampilan teknis administrator jaringan, beberapa program pelatihan keamanan jaringan berbasis Mikrotik telah diluncurkan. Kegiatan ini meningkatkan pertahanan jaringan banyak organisasi terhadap serangan siber, yang pada gilirannya meningkatkan perlindungan data dan efisiensi operasional di tempat kerja. Meskipun demikian, jumlah karya ilmiah yang dipublikasikan mengenai Praktik Kerja Lapangan dalam konteks keamanan jaringan berbasis Mikrotik sangat terbatas. Oleh karena itu, penelitian tambahan diperlukan untuk mencatat hasil implementasi ini dalam Praktik Kerja Lapangan dan bagaimana hal itu berdampak pada efektivitas dan keamanan jaringan di berbagai industri.

3. METODE PENGABDIAN MASYARAKAT

Dalam bagian ini, proses Praktik Kerja Lapangan terkait pengelolaan jaringan di lingkungan Dinas Komunikasi, Informatika, dan Statistik Provinsi NTB dijelaskan dengan menggunakan perangkat Mikrotik. Saya berpartisipasi sebagai partisipan utama dalam kegiatan ini, didampingi oleh tiga penanggung jawab divisi, dan dibimbing oleh Bapak Danny Ilham Iswara. Kegiatan ini mencakup analisis kebutuhan jaringan untuk menemukan masalah jaringan saat ini. Identifikasi solusi teknologi dan pilih konfigurasi mikrotik terbaik. Konfigurasi awal DHCP server dan firewall untuk keamanan jaringan. Periksa koneksi dan perbaiki jika perlu. Setiap langkah implementasi dicatat dalam dokumentasi dan pelaporan hasil. Untuk menilai efektivitas konfigurasi Laporan dibuat untuk dokumentasi internal. Proses implementasi praktik lapangan yang berkaitan dengan pengelolaan jaringan dengan Mikrotik digambarkan di bawah ini:



Gambar 1. Diagram Alur Praktik Kerja Lapangan

3.1. Tahap Analisis Kebutuhan Jaringan di Lingkungan Kominfo

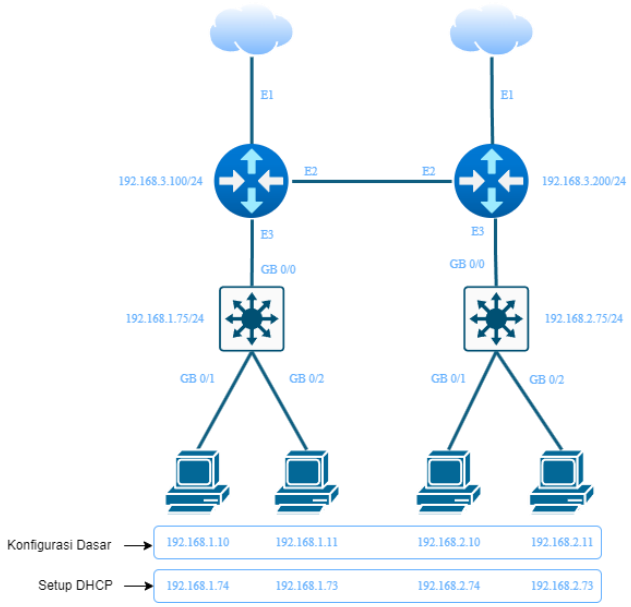
Tahap pertama yang dilakukan dalam pelaksanaan Praktik Kerja Lapangan ini adalah melakukan analisis terhadap kondisi jaringan di lingkungan Kominfo. Berdasarkan observasi dan wawancara dengan tim pengelola jaringan, ditemukan beberapa kendala utama yang terdiri dari distribusi alamat *IP* yang tidak efisien, yang mengakibatkan konflik *IP* antara pengguna, kontrol keamanan jaringan yang terbatas, sehingga rentan terhadap serangan atau akses tidak sah dan pemanfaatan perangkat jaringan yang kurang optimal, terutama dalam hal manajemen *routing*. Analisis ini bertujuan untuk memahami permasalahan yang ada dan menentukan kebutuhan spesifik yang harus dipenuhi untuk meningkatkan performa dan keamanan jaringan. Fokus utama pada tahap ini adalah bagaimana menerapkan solusi yang efektif melalui konfigurasi dasar, pengaturan *DHCP server*, dan implementasi *firewall* pada Mikrotik.

3.2. Identifikasi Solusi Teknologi

Setelah analisis kebutuhan dilakukan, solusi teknologi yang relevan diidentifikasi. Dalam hal ini, perangkat MikroTik dipilih karena memiliki kemampuan untuk mengatasi permasalahan jaringan yang ditemukan di Kominfo. Solusi ini mencakup beberapa aspek penting, Pertama akan melakukan konfigurasi dasar diikuti dengan pengaturan *IP address* statis dan dinamis, konfigurasi *routing* dasar, pengaturan *DNS*, dan penerapan *masquerade* untuk mengatasi kebutuhan *NAT* (*Network Address Translation*). Kedua, akan mengimplementasikan *DHCP Server* yang nantinya Mikrotik akan digunakan untuk mengelola *DHCP server* yang dapat mendistribusikan alamat *IP* secara otomatis kepada perangkat dalam jaringan. Hal ini membantu mengurangi risiko konflik *IP* dan mengoptimalkan penggunaan *IP address*. Terakhir yaitu pengaturan *firewall* Mikrotika yang akan dikonfigurasikan untuk melindungi jaringan dari ancaman eksternal, seperti serangan *DDoS* dan *malware*. Konfigurasi *firewall* juga mencakup pembuatan kondisi untuk membatasi akses yang tidak diinginkan.

3.3. Implementasi Konfigurasi MikroTik

Tahap ini mencakup implementasi solusi yang telah diidentifikasi. Proses implementasi dibagi menjadi beberapa langkah utama, Pada konfigurasi dasar jaringan akan dilakukan penambahan alamat *IP*, *routing*, *DNS*, dan *masquerade* dilakukan untuk memastikan konektivitas jaringan berjalan dengan baik. Pada implementasi *DHCP Server* dikonfigurasikan untuk mendistribusikan *IP address* secara otomatis. Parameter seperti *IP pool* dan *lease time* juga diatur untuk memastikan efisiensi distribusi. Sementara pada konfigurasi *firewall* pengaturan yang dilakukan dengan membuat pembatasan *action* dan pembutan kondisi untuk melindungi jaringan dari ancaman eksternal.



Gambar 2. Topologi Jaringan Mikrotik

Pada gambar topologi diatas akan dijadikan refrensi jaringan topologi dalam perancangan dan penggunaan semua metode-metode yang akan digunakan akan memiliki topologi jaringan yang sama dengan tujuan pembaca lebih memahami penerapan dalam konfigurasi jaringan didalam Mikrotik.

3.4. Dokumentasi dan Pelaporan

Tahap terakhir dalam kegiatan Praktik Kerja Lapangan ini adalah melakukan dokumentasi dan pelaporan hasil implementasi. Dokumentasi meliputi hasil konfigurasi di mana setiap langkah konfigurasi, mulai dari pengaturan *IP address*, implementasi *DHCP server*, hingga konfigurasi *firewall*, didokumentasikan secara detail. Hasil konfigurasi jaringan akan diberikan bukti setelah konfigurasi selesai berupa hasil yang juga mencakup pengujian fungsi dari konfigurasi yang telah dilakukan untuk memastikan sistem berjalan sesuai dengan yang diharapkan. Pengujian dilakukan untuk memastikan distribusi *IP* berjalan lancar dan *firewall* berfungsi dengan baik. Dan dokumentasi Kegiatan Praktik Kerja Lapangan (PKL), dokumentasi ini berisi foto-foto dan laporan kegiatan mengenai tahapan praktik lapangan yang telah dilaksanakan di Kominfo.

Laporan ini akan diserahkan kepada pihak Universitas Mataram sebagai bentuk pertanggungjawaban atas pelaksanaan kegiatan Praktik Kerja Lapangan, serta sebagai acuan bagi pengelola jaringan di Kominfo untuk melakukan perawatan dan pengembangan sistem di masa mendatang.

4. HASIL DAN PEMBAHASAN

Perancangan Mikrotik secara virtual dilakukan menggunakan beberapa alat bantu seperti VMware, Pnetlab, dan Winbox. VMware digunakan untuk menjalankan mesin virtual, tempat di mana *RouterOS* Mikrotik versi 6.49.10 diinstal. VMware memungkinkan simulasi jaringan tanpa perlu perangkat fisik. Setelah mesin virtual siap, Pnetlab digunakan sebagai *platform* untuk merancang topologi jaringan secara virtual. Pnetlab memudahkan pembuatan dan pengelolaan jaringan yang kompleks melalui perangkat virtual seperti *router* dan *switch*, yang kemudian dapat dihubungkan untuk mensimulasikan jaringan nyata.

Untuk konfigurasi, Winbox digunakan sebagai alat yang memudahkan pengguna dalam mengelola pengaturan *RouterOS* Mikrotik. Winbox menyediakan antarmuka grafis yang intuitif, memungkinkan pengelolaan fitur-fitur seperti *IP routing*, *firewall*, *NAT*, dan lainnya. *File ISO* Mikrotik, yang merupakan sistem operasi *RouterOS*, bertindak sebagai *router* virtual di lingkungan mesin virtual ini, sehingga pengguna dapat melakukan pengujian dan konfigurasi jaringan secara menyeluruh sebelum diterapkan di perangkat fisik.

4.1. Konfigurasi Dasar

Dalam konteks jaringan menggunakan perangkat MikroTik adalah langkah awal untuk mengatur perangkat agar bisa berfungsi dengan baik dalam suatu jaringan. Konfigurasi ini meliputi pengaturan dasar yang diperlukan untuk memastikan perangkat dapat mengelola lalu lintas data, mengalokasikan alamat *IP*, serta memberikan akses yang aman dan stabil kepada pengguna jaringan yang akan dijelaskan sebagai berikut ini.

```
[admin@Gedung_B] > ip route add dst-address=192.168.1.0/24 gateway=192.168.3.100
[admin@Gedung_B] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADS  0.0.0.0/0                          10.0.137.1                1
 1 ADC  10.0.137.0/24      10.0.137.139    ether1                    0
 2 A S  192.168.1.0/24                     192.168.3.100             1
 3 ADC  192.168.2.0/24     192.168.2.75    ether3                    0
 4 ADC  192.168.3.0/24     192.168.3.200   ether2                    0

[admin@Gedung_A] > ip firewall nat add chain=srcnat out-interface=ether1 \
\... action=masquerade
[admin@Gedung_A] > ip firewall  nat print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=srcnat action=masquerade out-interface=ether1
[admin@Gedung_A] >
```

Gambar 3. Konfigurasi *IP Address*, *Routing* dan *Network Address Translation*

Dalam proses awal konfigurasi adalah pembuatan *IP Address* dengan cara menuliskan perintah "ip address add address=192.168.x.x/x interface=ether_x" dan menulisakan perintah "ip address print" untuk memastikan apakah *IP Address* yang ditambahkan sudah terdapat pada Mikrotik. Dengan konfigurasi ini, perangkat dalam jaringan mendapatkan alamat IP yang sesuai, memastikan komunikasi antarperangkat berjalan lancar dan stabil. Selanjutnya adalah pembuatan *IP Route* dengan cara menulisakan perintah "ip route add dst-address=192.168.x.0 gateway=192.168.x.x" dengan tujuan Mikrotik dan *Server* 1 dan 2 bisa saling terhubung dan melakukan *ping* antar satu sama lain dan routing yang tepat mengoptimalkan aliran data di jaringan, mencegah kemacetan, dan memastikan konektivitas antarperangkat tanpa gangguan. Bagian selanjutnya adalah pembuatan *NAT* (*Network Address Translation*) yang berguna menyembunyikan *IP Adsress* pada setiap paket data yang keluar dari lokal *user*. Karena *router* berada diantara jaringan publik (internet) dan jaringan lockal (*LAN*), dengan cara "ip firewall nat add chain=srcnat out-interface-ether_x action=masquerade". Penerapan NAT meningkatkan keamanan dengan melindungi identitas IP internal serta memungkinkan berbagi koneksi internet dengan lebih efisien.

4.2. IP DHCP Server

Pada peroses awal yang perlu dilakukan dalam metode *IP DHCP* adalah melakuakn konfigurasi dasar seperti sebelumnya yaitu penambahan *IP Address*, *Route*, *DNS* dan *NAT*. Namun tidak perlu melakuakan penambahan *IP Address* secara manual pada *PC*, pada tahap itu silahkan dilewatkan dikarenakan *IP DHCP* nantinya akan menambahkan *IP* Address pada tiap-tiap *PC* secara otomatis yang akan dijelaskan sebagai berikut.

```
[admin@Gedung_A] > ip dhcp-server lease add address=192.168.1.73 \
\... mac-address=00:50:79:66:68:06
[admin@Gedung_A] > ip dhcp-server lease print
Flags: X - disabled, R - radius, D - dynamic, B - blocked
 #    ADDRESS         MAC-ADDRESS       H SE.. R STATUS   LAST-SEEN
 0 D 192.168.1.74    00:50:79:66:68:05 V dh..   bound    14m48s
 1   192.168.1.73    00:50:79:66:68:06          waiting never
```

	Address	MAC Address	Client ID	Server	Active Address	Active MAC Addre...	Active Hos...	Expires After	Status
	192.168.1.73	00:50:79:66:68:06		all					waiting
D	192.168.1.74	00:50:79:66:68:05	1:0:50:79:66:68:5	dhcp1	192.168.1.74	00:50:79:66:68:05	VPCS1	00:28:33	bound

```
[admin@Gedung_A] > ip dhcp-server set dhcp1 add-arp=yes
[admin@Gedung_A] > interface ethernet set ether3 arp=reply-only
```

Gambar 4. Konfigurasi *DHCP Server, Static Mapping* dan Pengamanan *DHCP Server*

Untuk melakukan konfigurasi *DHCP server* pada *interface* yang digunakan dapat dilakukan pada *wizard* yang sudah disediakan dengan menulis perintah "ip dhcp-server setup" lalu memilih *interface* mana yang akan digunakan "ether_x" diikuti penambahan address space "192.168.x.0/24" dan pemilihan gateway "192.168.x.x" dan address yang akan diberikan dari mana hingga mana "192.168.x.1-192.168.x.10" menentukan DNS server "192.168.x.x, 192.168.x.x" terakhir menetukan lease time "30m" lalu untuk melihat detail dapat dilakukan dengan menulis perintah "ip dhcp-server print detail" atau "ip dhcp-server network print detail". memilih interface, menentukan range IP, dan mengatur lease time. DHCP server memastikan setiap perangkat mendapatkan IP secara otomatis, sehingga administrator tidak perlu mengonfigurasi satu per satu, menghemat waktu dan meminimalkan kesalahan.

Selanjutnya akan melakukan Static Mapping yang bertujuan memastikan apabila *IP Address* tertentu telah digunakan, maka *IP Address* tersebut tidak akan digunakan oleh komputer *user* lain dengan menuliskan perintah "ip dhcp-server lease add address=192.168..x.x mac-address=x:x:x:x:x:x". mac-address yang sudah aktif dapat dilihat dengan menggunakan perintah "ip dhcp-server lease print" atau "ip dhcp-server lease print detail". Dapat dilihat setelah melakukan static mapping maka PC yang memiliki IP Address "192.168.1.73" tidak perlu menunggu

untuk mendapatkan IP karena telah memilki IP tetap. Static mapping penting dalam mengamankan dan mengontrol perangkat dalam jaringan agar tidak terjadi konflik IP yang dapat mengganggu konektivitas.

Sebenarnya *IP DHCP* sudah dapat digunakan pada tiap *PC* yang terhubung pada Mikrotik namun tedapat juga cara pengamanan yang dapat dilakukan dengan *DHCP Server* dengan tujuan sebagai pengawasan jaringan, agar komputer *user* 'jahat' tidak dapat menghubungkan komputernya ke dalam Mikrotik "ip dhcp-server set dhcp1 add-arp=yes" dan "interface ethernet set ether_x arp=reply-only". Langkah ini meningkatkan keamanan dengan membatasi akses hanya untuk perangkat yang terdaftar.

4.3. Konfigurasi Firewall

Pada peroses awal yang perlu dilakukan adalah melakuakn konfigurasi dasar seperti sebelumnya yaitu penambahan *IP Address*, *Route*, *DNS*, *NAT* dan juga pembutan *IP Address* pada tiap *PC* yang digunakan boleh secara manual atau *IP DHCP*. Pada bagian awal *firewall* perlu diketahui bahwa terdapat 3 *action* yaitu *accep*t, *drop*, dan *reject*. *Accept* merupakan *action* yang digunakan untuk meloloskan paket data yang akan menuju internet. *Drop* merupakan *action* yang digunakan untuk membuang paket data yang akan menuju internet. Dan terakhir *reject* memiliki tujuan yang sama dengan *action drop* hanya saja memberikan pesan *error* pada komputer *user* sementara untuk perancangannya sendiri akan dijelaskan sebagai berikut.

```
[admin@Gedung_A] > ip firewall filter add chain=forward src-address=192.168.1.74 \

\... action=drop
[admin@Gedung_A] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=forward action=accept src-address=192.168.1.0/24
      dst-address=192.168.2.0/24

 1    chain=forward action=accept src-address=192.168.2.0/24
      dst-address=192.168.1.0/24

 2    chain=forward action=drop src-address=192.168.1.74
```

Gambar 5. Konfigurasi *Action Address*

Pada parameter *src-address* dapat digunakan untuk pembatasan internet dengan cara menuliskan perintah "ip firewall filter add chain=forward src-address=192.168.x.x action=drop", pada bagian *action* dapat diganti menjadi *reject* atau *accept*. Untuk melihat detail dapat menuliskan "ip firewall filter print". Dengan aturan ini, akses jaringan dapat dikontrol, mencegah aktivitas mencurigakan yang berpotensi merugikan sistem.

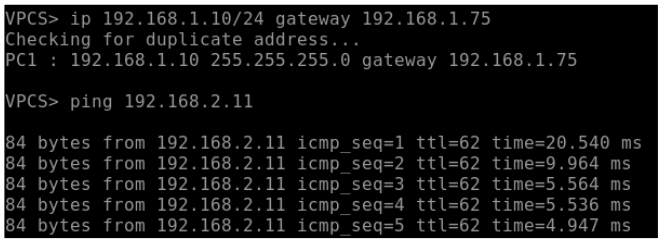
```
[admin@Gedung_B] > ip firewall filter add chain=forward src-address=192.168.2.1-19
2.168.2.10 time=08:00:00-11:00:00,mon,tue,wed action=reject
[admin@Gedung_B] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=forward action=accept src-address=192.168.1.0/24
      dst-address=192.168.1.0/24

 1    chain=forward action=accept src-address=192.168.1.0/24
      dst-address=192.168.2.0/24

 2 I  ;;; inactive time
      chain=forward action=reject src-address=192.168.2.1-192.168.2.10
      time=8h-16h,mon,tue,wed

 3 I  ;;; inactive time
      chain=forward action=reject src-address=192.168.2.1-192.168.2.10
      time=8h-11h,mon,tue,wed
```

Gambar 6. Konfigurasi *Action Address* dengan Kondisi

Filter ini juga terdapat berbagai macam cara lainnya contohnya dengan parameter time dengan menuliskan perintah "ip firewall filter add chain=forward src-address=192.168.x.x-192.168.x.x time=08:00:00-16:00:00, mon, tue,wed,thu, fri,sat,sun action=drop" atau dengan filter HTTP dan HTTPS dengan menuliskan perintah "ip firewall filter add chain=forward src-address=192.168.x.x protocol=tcp dst-port=80 action=drop", lalu yang menyerupai terdapat filter *DNS* (*Domain Name System*) "ip firewall filter add chain=forward src-address=192.168.x.x/24 protocol=udp dst-port=53 action=drop". Penerapan aturan tambahan dapat dilakukan berdasarkan waktu atau protokol tertentu. Ini membantu dalam membatasi akses berdasarkan kebijakan organisasi, seperti membatasi akses ke situs tertentu selama jam kerja.

4.4. Hasil Pengujian

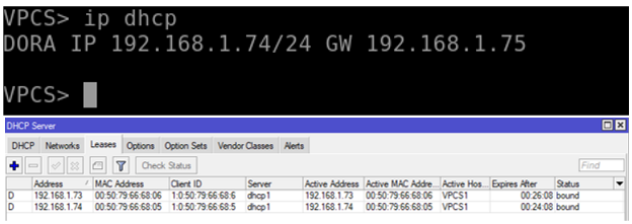
a. Hasil Konfigurasi Dasar



Gambar 7. Konfigurasi *PC* Manual

Bagian terakhir dari konfigurasi dasar adalah penambahan secara *IP Address* pada *PC* secara manual dengan menuliskan perintah "ip address 192.168.x.x/24 gateway 192.168.x.x" dan seluruh PC yang terhubung dari kedua Mikrotik yang ada, akan saling terhubung dengan satu sama lain contohnya seperti pada gambar *PC*1 memiliki *IP Address* "192.168.1.10/24" melakukan *ping* ke *PC*4 dengan *IP Adddres* "192.168.2.11/24" dan dapat dilihat bahwa kedua *PC* tersebut saling terhubung. menunjukkan bahwa perangkat dalam jaringan dapat saling terhubung tanpa kendala, meningkatkan efisiensi komunikasi dan memastikan stabilitas jaringan dalam operasional harian.

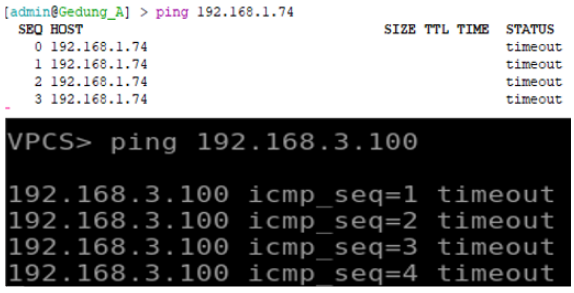
b. Hasil Konfigurasi *DHCP Server*



Gambar 8. Konfigurasi Pengaturan *IP DHCP* Pada *PC*

Hasil akhir untuk memastikan apakah *IP DHCP* berhasil dapat menulis perintah pada *PC* yaitu "*IP DHCP*" apabila muncul/terdapat kata "*DORA*" ketika melakukan konfigurasi, maka *IP Address* dan *Gateway* akan dibuat secara otomatis tanpa penulisan secara manual. Untuk melihat *IP Address* yang mana saja sudah dipinjamkan dapat dilihat melalui WinBox dan membuka menu IP > DHCP Server > tab Leases. Hal ini memastikan efisiensi dalam pengelolaan jaringan, menghindari kesalahan manusia dalam pemberian alamat IP.

c. Hasil Konfigurasi Firewall



Gambar 9. Hasil Konfigurasi *Firewall*

Hasil akhir untuk memastikan apakah *Firewall* berhasil dapat melakukan dilakukanya *ping* dari komputer ke Mikrotik yang diberikan penghalang *Firewall* dalam mengakses jaringan internet. Dengan menuliakan perintah "ping 192.168.x.x" dan dapat disimpulkan filter *Firewall* berhasil diterapkan pada Mikrotik dengan *IP* "192.168.3.100" dan *PC* dengan IP "192.168.1.74" tidak saling terhubing. Hasil menunjukkan bahwa aturan firewall berhasil diterapkan, memberikan kontrol lebih terhadap lalu lintas jaringan, meningkatkan keamanan, dan mencegah akses tidak sah.

Analisis Dampak Implementasi Mikrotik menunjukkan bahwa pengelolaan jaringan di Kominfo NTB menjadi lebih baik. DHCP meningkatkan efisiensi dengan mengotomatiskan alokasi IP, dan firewall meningkatkan keamanan dengan menghentikan akses yang tidak diinginkan. Selain itu, implementasi ini mempermudah

manajemen jaringan, mengurangi kemungkinan kesalahan konfigurasi, dan meningkatkan keandalan dan stabilitas jaringan. Pengelolaan jaringan yang lebih efektif membantu Kominfo NTB karena mengurangi waktu yang dibutuhkan untuk konfigurasi dan pemeliharaan. Adanya firewall dan DHCP server yang berfungsi dengan baik mengurangi kemungkinan gangguan jaringan karena akses tidak sah dan konflik IP. Hal ini langsung berdampak pada peningkatan efisiensi pegawai dan memastikan bahwa layanan digital Kominfo NTB berjalan dengan aman dan optimal. Jadi, teknologi ini meningkatkan kinerja jaringan dan perlindungan data di Kominfo NTB.

4.5. Dokumentasi Praktek Kerja Lapangan

Gambar 10. Kantor Kominfo

Pada gambar di atas menunjukkan lokasi Kantor Kominfo, tempat dimana menjalani praktik kerja lapangan. Kantor Kominfo (Kementerian Komunikasi dan Informatika) merupakan instansi pemerintah daerah yang berada di bawah naungan Kementerian Komunikasi dan Informatika Indonesia. Instansi ini bertugas mengelola, mengembangkan, dan mengawasi kebijakan-kebijakan terkait komunikasi dan informasi di wilayah Kota Mataram.

Gambar 11. Proses Penyerahan Tugas

Selain menjadi tempat praktik, kantor ini juga menjadi ruang diskusi dan evaluasi, di mana setiap tugas yang diselesaikan mendapat tinjauan serta masukan yang membangun. Hal ini sangat membantu dalam meningkatkan pemahaman terkait tugas-tugas yang berkaitan dengan pengelolaan, pengembangan, dan pengawasan kebijakan-kebijakan komunikasi dan informasi di wilayah Kota Mataram, yang merupakan fokus dari Kantor Kominfo.

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan apa yang telah disebutkan di atas, Mikrotik memberikan banyak keuntungan teknis untuk penggunaan dalam pengelolaan jaringan, serta meningkatkan efisiensi kerja dan keamanan jaringan. Fiturnya, seperti konfigurasi IP address, routing, NAT, dan implementasi DHCP server, memungkinkan pengelolaan jaringan yang lebih otomatis dan terstruktur, yang mengurangi kemungkinan kesalahan konfigurasi dan meningkatkan stabilitas koneksi. Dari perspektif keamanan, pengaturan firewall yang tepat memungkinkan jaringan dilindungi dari ancaman luar dan memberikan kontrol lalu lintas data yang lebih baik, yang secara langsung berkontribusi pada perlindungan data dan kelangsungan operasional sistem. Selain itu, integrasi yang mudah dengan aplikasi seperti VMware, Pnetlab, dan Winbox memungkinkan simulasi dan pengujian sebelum implementasi nyata, yang memungkinkan administrator untuk menemukan dan mengatasi masalah yang mungkin lebih awal. Secara keseluruhan, Mikrotik meningkatkan kinerja jaringan dan membantu tim IT bekerja lebih efisien dengan sistem yang lebih mudah dikelola dan lebih aman dari gangguan.

5.2. Saran

Untuk memaksimalkan pemanfaatan Mikrotik dalam manajemen jaringan, ada beberapa saran dapat diterapkan atau dilakukan dalam memaksimumkan fungsi dan metode dari Mikrotik. Terapkan standar keamanan yang lebih ketat melalui konfigurasi *firewall* dan enkripsi yang lebih kuat, terutama di jaringan yang terhubung dengan internet publik. Sebelum melakukan perubahan besar pada jaringan, manfaatkan aplikasi pendukung seperti VMware dan PnetLab untuk melakukan simulasi dan pengujian agar meminimalkan kesalahan konfigurasi.

UCAPAN TERIMA KASIH

Penelitian ini tidak akan mungkin tercapai tanpa dukungan dan bantuan dari berbagai pihak. Oleh karena itu, penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada, Bapak Danny Ilham Iswara pembimbing yang telah memberikan bimbingan, arahan, dan dukungan yang tak ternilai sepanjang proses ini. Masukan dan saran mereka sangat berharga dalam setiap tahap penyusunan jurnal ini, dan juga departemen Teknik Informatika, Universitas Mataram, serta Dinas Komunikasi Informatika dan Statistik Prov NTB yang telah menyediakan fasilitas serta lingkungan akademik yang mendukung untuk pengerjaan jurnal ini. Terima kasih atas semua dukungan yang diberikan, dan Keluarga serta Sahabat, yang selalu memberikan doa, dukungan moral, dan motivasi tanpa henti. Terima kasih kepada orang tua, saudara, dan teman-teman dekat yang telah memberikan dukungan emosional dan mental selama masa-masa sulit dalam pengerjaan jurnal ini.

Akhir kata, penulis menyadari bahwa jurnal ini masih memiliki banyak kekurangan. Oleh karena itu, saran dan kritik yang membangun sangat diharapkan untuk perbaikan di masa mendatang. Semoga hasil penelitian ini dapat memberikan manfaat yang besar bagi perkembangan ilmu pengetahuan dan teknologi, khususnya dalam bidang jaringan dan keamanan. Terima kasih.

DAFTAR PUSTAKA

[1] Permadi dan S. Kusumah, "Efisiensi Penggunaan Mikrotik dalam Pengelolaan Jaringan," *Jurnal Teknologi Informasi dan Komputer*, vol. 10, no. 2, pp. 55-63, 2021.
[2] Priyanto, A. (2019). *Analisis Implementasi MikroTik dalam Pengelolaan Jaringan di Lembaga Pemerintah*. Journal of Network Security, 12(3), 44-58.
[3] Y. Pratama dan N. A. Wibowo, "Pengaturan IP Address dan Gateway pada Mikrotik untuk Jaringan Dasar," Jurnal Sistem Komputer, vol. 13, no. 2, pp. 45-52, 2021.
[4] A. Siregar dan F. Widodo, "Konfigurasi Mikrotik Sebagai Router Dasar untuk Jaringan LAN," Jurnal Teknologi Informasi, vol. 10, no. 1, pp. 12-19, 2020.
[5] F. Lestari, "Implementasi Konfigurasi Mikrotik untuk Pengaturan Bandwidth Menggunakan Simple Queue," *Jurnal Sistem Komputer*, vol. 9, no. 2, pp. 34-40, 2020.
[6] H. Wijaya dan R. Hidayat, "Implementasi DHCP Server Menggunakan Mikrotik pada Jaringan Kampus," *Jurnal Sistem Informasi*, vol. 14, no. 3, pp. 89-97, 2020.
[7] S. Hartono dan D. Wibowo, "Implementasi DHCP Server Menggunakan Mikrotik pada Jaringan Skala Kecil," Jurnal Jaringan dan Komunikasi, vol. 7, no. 2, pp. 56-63, 2021.
[8] I. Anshori dan S. Riyadi, "Penggunaan Mikrotik dalam Pengaturan DHCP Server untuk Optimalisasi Pengelolaan IP Address di Perusahaan," *Jurnal Teknologi Informasi dan Komunikasi*, vol. 15, no. 1, pp. 101-110, 2020.
[9] S. Kurniawan dan D. Utami, "Penerapan DHCP Server Berbasis Mikrotik untuk Mengelola Distribusi IP pada Sekolah Menengah Atas," *Jurnal Teknologi Pendidikan*, vol. 17, no. 4, pp. 74-83, 2021.
[10] N. Kurniawan dan R. Hidayat, "Optimalisasi Pengelolaan DHCP Server pada Mikrotik Router untuk Mengatasi Masalah IP Conflict," *Jurnal Informatika dan Jaringan*, vol. 11, no. 2, pp. 28-36, 2020.
[11] M. Rahman dan I. Setiawan, "Analisis Keamanan Firewall Mikrotik dalam Mengatasi Serangan Siber," *Jurnal Keamanan Jaringan*, vol. 8, no. 1, pp. 102-110, 2019.
[12] M. Faizal dan A. Permana, "Perancangan dan Konfigurasi Mikrotik Firewall untuk Mengamankan Jaringan Internal," Jurnal Teknik Informatika dan Sistem Informasi, vol. 9, no. 3, pp. 111-118, 2019.
[13] F. Nugroho dan R. Putra, "Konfigurasi Firewall Mikrotik untuk Mencegah Akses yang Tidak Diinginkan di Jaringan Publik," Jurnal Keamanan Jaringan, vol. 8, no. 4, pp. 85-92, 2021.
[14] M. Rasyid dan A. Zulkarnain, "Konfigurasi Firewall pada Mikrotik untuk Menyaring Lalu Lintas Data Berbahaya," *Jurnal Teknologi Jaringan*, vol. 6, no. 3, pp. 67-75, 2020.
[15] R. Widodo, "Analisis Penggunaan Firewall Mikrotik dalam Meningkatkan Keamanan Jaringan di Perusahaan," *Jurnal Teknologi dan Keamanan Jaringan*, vol. 10, no. 2, pp. 50-60, 2021.