**TUGAS AKHIR**

**PERANCANGAN DAN IMPLEMENTASI AUTOMATIC FAILOVER DAN METODE FIREWALL FILTERING PADA KEAMANAN JARINGAN BERBASIS MIKROTIK**

Sebagai Syarat untuk Mendapatkan Gelar Sarjana Program Studi Teknik Industri.

Strata 1 (S-1)



**DISUSUN OLEH:**

**NAMA : ENGGAR RIANTO**

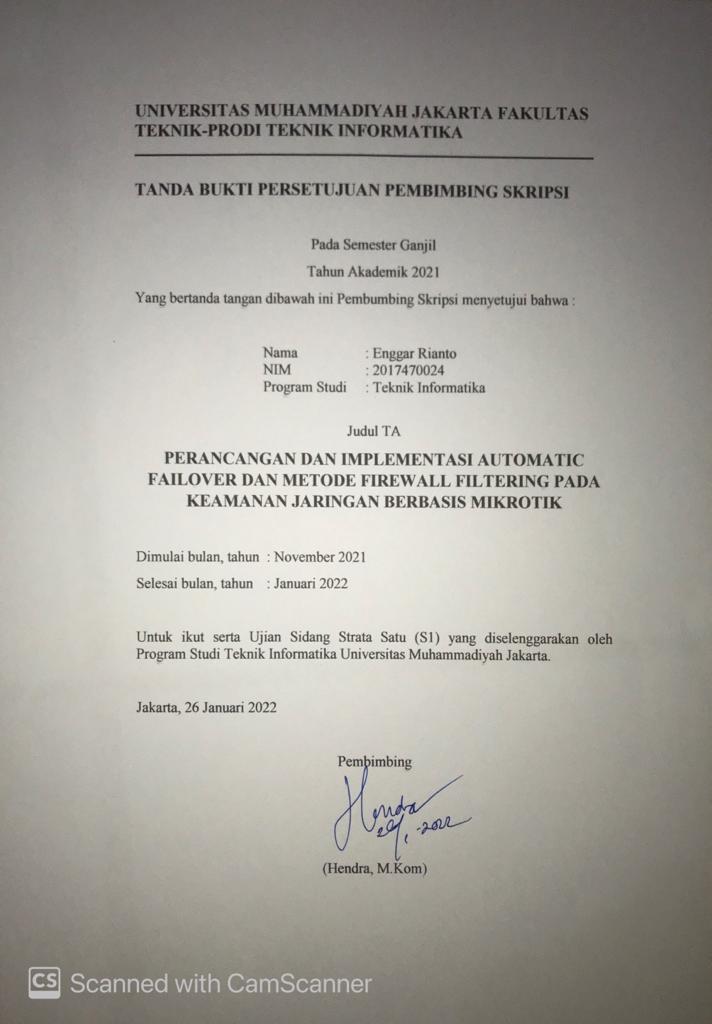
**NPM : 2017470024**

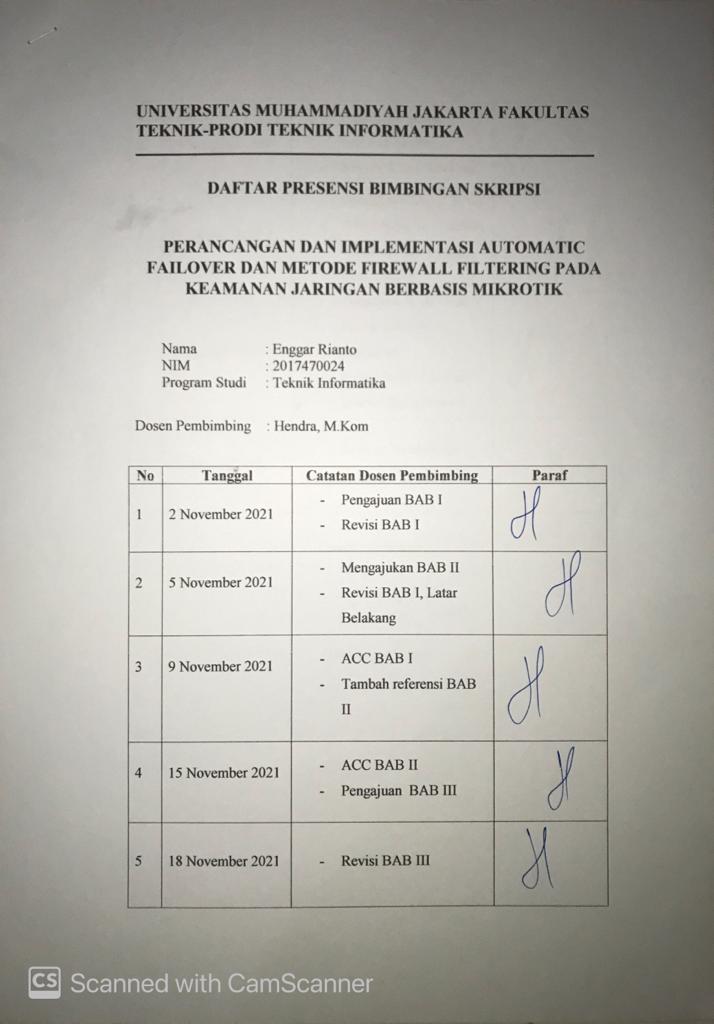
**PROGRAM STUDI TEKNIK INFORMATIKA**

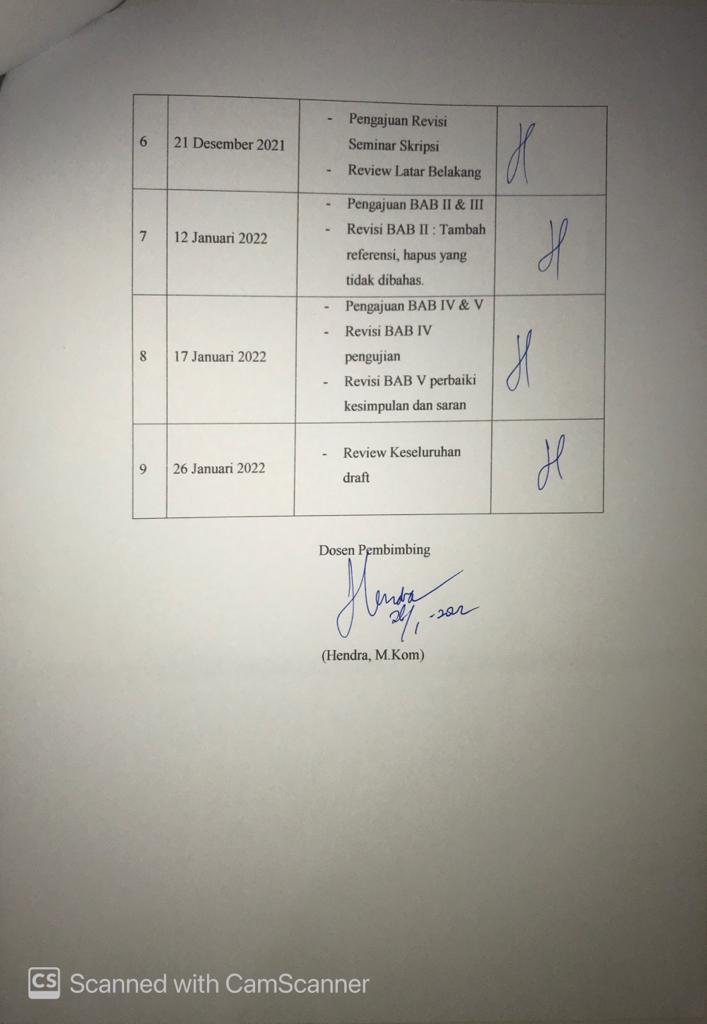
**FAKULTAS TEKNIK**

**UNVERSITAS MUHAMMADIYAH JAKARTA**

**2023**

****

****

****

# **ABSTRAK**

Pertumbuhan penggunaan jaringan internet di Indonesia saat ini sangat signifikan. Saat ini banyak pengguna yang memakai lebih dari 1 ISP untuk memenuhi kebutuhannya. Permasalahan yang sering terjadi adalah ketika salah satu koneksi internet terputus, maka pengguna harus mengganti koneksi ke ISP lainnya agar bisa terhubung kembali. Untuk mengatasi hal tersebut, diperlukannya suatu koneksi backup apabila putus koneksi pada koneksi utama, maka koneksi *backup* akan menjalankan fungsinya menggantikan koneksi utama secara otomatis. Metode tersebut itulah yang dinamakan dengan *automatic failover* koneksi yang perlu diterapkan. Metode ini menggunakan 2 ISP dan menjadikan Mikrotik sebagai *automatic failover* hal ini berfungsi untuk mengoptimalkan *failover* saat terjadi putus koneksi pada *link* ISP utama. Pada penelitian terdahulu tentang implementasi *automatic failover* terdapat kekurangan seperti *automatic failover* hanya bekerja saat jalur koneksi mikrotik ke modem ISP terputus. Pada penelitian ini dibuat pengembangan *automatic failover* menggunakan dua  *line* ISP dengan *recursive gateway*. *Automatic* *failover* dengan *recursive gateway* ini diimplementasikan menggunakan perangkat *Mikrotik*. Dengan *Recursive gateway* ini pengecekan *gateway* lebih efektif dibandingkan dengan cara mengecek *gateway* hanya sebatas pada IP modem, sehingga dapat terdeteksi ketersediaan koneksi pada masing-masig ISP. F*irewall filtering* dengan pembatasan IP untuk kemanan jaringan, agar tidak dapat diakses oleh pengguna lain. Hasil pengujian menunjukkan perpindahan *link* secara otomatis dengan melakukan pengecekan ke *gateway* ISP, sehingga tidak perlu mengganti secara manual. Hasil pengujian keamanan jaringan, IP *user* selain admin tidak dapat mengakses Mikrotik dan admin mendapatkan notifikasi jika terdapat user yang mencurigakan mengakses jaringan.

Kata kuncinya : *failover*, *firewall*, *recursive gateway*, keamanan jaringan, mikrotik

# **KATA PENGANTAR**

Puji syukur penulis panjatkan kehadirat Allah SWT atas Rahmat dan Hidayah-Nya, sehingga penyusun dapat menyelesaikan Skripsi dengan judul “ PERANCANGAN DAN IMPLEMENTASI AUTOMATIC FAILOVER DAN METODE FIREWALL FILTERING PADA KEAMANAN JARINGAN BERBASIS MIKROTIK“. Berkat doa, dorongan dan arahan dari berbagai pihak, sehingga semua kesulitan dan hambatan yang penulis hadapi dapat terselesaikan dengan baik.

Dalam kesempatan ini penyusun mengucapkan terimakasih yang sebesar- besarnya kepada pihak-pihak yang telah membantu dalam penyelesaian Skripsi ini, kepada :

1. Allah SWT, yang telah melimpahkan rahmat, kasih sayang, kesehatan dan hidayah-nya.
2. Ibu dan Bapak saya yang selalu memberikan dukungan semangat serta do’a restunya dalam menyelesaikan Skripsi ini.
3. Bapak Irfan Purnawan, S.T., M.Chem.Eng, selaku Dekan Fakultas Teknik Universitas Muhammadiyah Jakarta.
4. Ibu Rita Dewi Risanty, MMSI, selaku Ketua Program Studi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jakarta.
5. Bapak Hendra, M.Kom sebagai seorang Dosen Pembimbing yang selalu mengarahkan, membantu, dan saran dalam membuat Skripsi ini.
6. Teman-teman angkatan 2017 yang telah memberikan semangat dan nasihat agar penulis lancar dalam mengerjakan Skripsi ini.
7. Seluruh Staff dan pengajar Jurusan Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jakarta.
8. Dan semua pihak yang tidak bisa disebutkan oleh penulis yang membantu saat penulis menulis Skripsi ini.

Akhirnya dengan rendah hati Penulis menyadari bahwa sekalipun menginginkan suatu hasil yang baik, tentunya masih ada kekurangan pada Skripsi ini. Untuk itu, kepada semua pihak dapat memaklumi dan memberikan saran serta kritik yang membangun demi kesempurnaan Skripsi ini selanjutnya. Harapan penulis agar Skripsi ini dapat bermanfaat bagi para pembaca dan khususnya bagi penulis untuk menambah pengetahuan dan penelitian selanjutnya, Aamiin.

Jakarta, 26 Januari 2022

Penyusun

Enggar Rianto

# **DAFTAR ISI**

[**ABSTRAK** 5](#_Toc95921098)

[**KATA PENGANTAR** 6](#_Toc95921099)

[**DAFTAR ISI** 8](#_Toc95921100)

[**DAFTAR TABEL** 10](#_Toc95921101)

[**DAFTAR GAMBAR** 11](#_Toc95921102)

[**BAB I** 14](#_Toc95921103)

[**PENDAHULUAN** 14](#_Toc95921104)

[1.1 Latar Belakang 14](#_Toc95921105)

[1.2 Identifikasi Masalah 16](#_Toc95921106)

[1.3 Rumusan Masalah 16](#_Toc95921107)

[1.4 Batasan Masalah 17](#_Toc95921108)

[1.5 Tujuan dan Manfaat Penelitian 17](#_Toc95921109)

[1.6 Metodologi Penelitian 17](#_Toc95921110)

[1.7 Sistematika Penulisan 18](#_Toc95921111)

[**BAB II** 20](#_Toc95921112)

[**TINJAUAN PUSTAKA** 20](#_Toc95921113)

[2.1 Jaringan 20](#_Toc95921114)

[2.1.1 Klasifikasi Jaringan Komputer 20](#_Toc95921115)

[2.2 Topologi Jaringan 21](#_Toc95921116)

[2.2.1. Topologi Bus 22](#_Toc95921117)

[2.2.2. Topologi Ring 22](#_Toc95921118)

[2.2.3. Topologi Mesh 23](#_Toc95921119)

[2.2.4. Topologi Tree 24](#_Toc95921120)

[2.2.5. Topologi Star 24](#_Toc95921121)

[2.3. Media Transmisi 25](#_Toc95921122)

[2.3.1 Kabel Unshielded Twisted Pair (UTP) 26](#_Toc95921123)

[2.3.2 Kabel Shielded Twisted Pair (STP) 26](#_Toc95921124)

[2.4 Router 27](#_Toc95921125)

[2.5 Switch 28](#_Toc95921126)

[2.6 Network Interface Card (NIC) 28](#_Toc95921127)

[2.7 IP (Internet Protocol) Address 29](#_Toc95921128)

[2.8 Modem 30](#_Toc95921129)

[2.9 Mikrotik 30](#_Toc95921130)

[2.9 Firewall Filter Rules 30](#_Toc95921131)

[2.10 Address List 31](#_Toc95921132)

[2.11 Failover 31](#_Toc95921133)

[2.12 Winbox 31](#_Toc95921134)

[2.13 Gateway 32](#_Toc95921135)

[2.14 ISP (*Internet Service Provider*) 32](#_Toc95921136)

[**BAB III** 33](#_Toc95921137)

[**METODOLOGI PENELITIAN** 33](#_Toc95921138)

[3.1 Analisis Sistem Jaringan Berjalan 33](#_Toc95921139)

[3.1.1 Topologi Jaringan 33](#_Toc95921140)

[3.1.2 Hardware Dalam Jaringan 34](#_Toc95921141)

[3.1.3 Perangkat Lunak Pendukung 35](#_Toc95921142)

[3.2 Anaisis Permasalahan Sistem Jaringan Berjalan 35](#_Toc95921143)

[3.2.1 Analisis Automatic Failover 35](#_Toc95921144)

[3.2.2 Analisis Firewall Filtering 36](#_Toc95921145)

[3.3 Analisis Kebutuhan Jaringan 36](#_Toc95921146)

[3.3.1 Spesifikasi Kebutuhan Perangkat Lunak 36](#_Toc95921147)

[3.3.2 Spesifikasi Kebutuhan Perangkat Keras 37](#_Toc95921148)

[3.4 Sistem Jaringan Usulan 37](#_Toc95921149)

[3.4.1 Topologi Jaringan 37](#_Toc95921150)

[3.4.2 Pengalamatan IP Address 39](#_Toc95921151)

[3.4.3 Perancangan Automatic Failover dengan Rekursif Gateway 40](#_Toc95921152)

[3.4.4 Perancangan Notifikasi Untuk Admin 41](#_Toc95921153)

[3.5 Langkah-langkah Pengujian 41](#_Toc95921154)

[**BAB IV** 43](#_Toc95921155)

[**HASIL DAN PEMBAHASAN** 43](#_Toc95921156)

[4.1 Pembangunan Infrastruktur 43](#_Toc95921157)

[4.2 Konfigurasi Jaringan 43](#_Toc95921158)

[4.2.1 Interface 43](#_Toc95921159)

[4.2.2 Konfigurasi IP Address 44](#_Toc95921160)

[4.2.3 Konfigurasi Automatic Failover 44](#_Toc95921161)

[4.2.4 Konfigurasi Recursive Gateway 48](#_Toc95921162)

[4.2.5 Konfigurasi Keamanan Jaringan 49](#_Toc95921163)

[4.2.6 Konfigurasi Notifikasi Admin 50](#_Toc95921164)

[4.3 Pengujian dan Hasil 51](#_Toc95921165)

[4.3.1 Pengujian Automatic Failover dengan Recursive Gateway 51](#_Toc95921166)

[4.3.2 Pengujian Keamanan Jaringan 53](#_Toc95921167)

[4.3.3 Pengujian Notifikasi Admin 55](#_Toc95921168)

[**BAB V** 56](#_Toc95921169)

[**PENUTUP** 56](#_Toc95921170)

[5.1 Kesimpulan 56](#_Toc95921171)

[5.2 Saran 56](#_Toc95921172)

# **DAFTAR TABEL**

Tabel 3.1 Spesifikasi Mikrotik RB 2011UiAS-RM…………................. 32

Tabel 3.2 Spesifikasi Switch D-Link DGS-1016C …….......................... 32

Tabel 3.4 Pengalamatan IP Address ........................................................ 36

Tabel 4.2 Hasil Pengujian Automatic Failover........................................ 51

# **DAFTAR GAMBAR**

Gambar 2.1 Topologi Bus........................................................................... 20

Gambar 2.2 Topologi Ring.......................................................................... 21

Gambar 2.3 Topologi Mesh…………........................................................ 21

Gambar 2.4 Topologi Tree…...................................................................... 22

Gambar 2.5 Topologi Star.......................................................................... 23

Gambar 2.6 Kabel UTP…........................................................................... 24

Gambar 2.7 Kabel STP…........................................................................... 25

Gambar 2.8 Router….................................................................................. 25

Gambar 2.9 Switch……….......................................................................... 26

Gambar 2.10 Network Interface Card............................................................ 27

Gambar 3.1 Topologi jaringan berjalan…................................................... 31

Gambar 3.2 Topologi star pada automatic failover….................................. 33

Gambar 3.3 Firewall Filltering………........................................................ 34

Gambar 3.4 Topologi Jaringan Usulan........................................................ 36

Gambar 4.1 Topologi Jaringan Yang Digunakan........................................ 40

Gambar 4.2 Tampilan Interface List............................................................ 40

Gambar 4.3 IP Address……........................................................................ 41

Gambar 4.4 Konfigurasi Mangle Input ISP 1……...................................... 42

Gambar 4.5 Konfigurasi Mangle Input ISP 2……...................................... 42

Gambar 4.6 Konfigurasi Mangle Output ISP 1…….................................... 43

Gambar 4.7 Konfigurasi Mangle Output ISP 2............................................ 44

Gambar 4.8 Konfigurasi Mangle Prerouting............................................... 44

Gambar 4.9 Konfigurasi Mangle Prerouting............................................... 45

Gambar 4.10 Konfigurasi Recursive ISP Utama........................................... 45

Gambar 4.11 Konfigurasi Recursive ISP Backup…...................................... 46

Gambar 4.12 Konfigurasi Blokir Akses........................................................ 46

Gambar 4.13 Konfigurasi Blokir Ping………............................................... 47

Gambar 4.14 Konfigurasi Notifikasi Admin ……......................................... 47

Gambar 4.15 Pengujian Saat ISP Utama Tidak Mengalami Gangguan......... 48

Gambar 4.16 Pengujian Saat ISP Utama Mengalami Gangguan…………... 49

Gambar 4.17 Pengujian Akses Router dan Pengecekan Ping….................... 50

Gambar 4.18 Pengujian Akses Router dan Pengecekan Ping........................ 50

Gambar 4.19 Hasil Notifikasi Admin………………………........................ 50

# **BAB I**

# **PENDAHULUAN**

## 1.1 Latar Belakang

Perkembangan teknologi, khususnya teknologi informasi menunjukan kemajuan yang pesat, baik di bidang perangkat keras maupun perangkat lunak. Perkembangan teknologi tersebut juga mempengaruhi cara manusia untuk berkomunikasi. Perkembangan telekomunikasi di masa sekarang yang modern ini, khususnya pada jaringan komputer, telah menjadi salah satu hal yang mendasar dalam kehidupan saat ini.

Kemajuan teknologi yang sangat pesat dan penyebaran koneksi internet yang tersebar begitu luas, membuat permintaan akan koneksi internet dengan kecepatan tinggi dan dapat diandalkan meningkat. LAN adalah singkatan dari *Local Area Network*. LAN terdiri dari beberapa komputer yang terhubung dalam suatu jaringan. Pada jaringan ini, setiap komputer yang terhubung ke jaringan dapat mengakses data dari komputer lain. Selain itu, komputer dapat mengakses data dari komputer lain. Setiap komputer yang terhubung pada LAN mempunyai IP Address yang berbeda. (Haryanto, 2012)

Pada jaringan, *switch* adalah alat untuk menghubungkan sejumlah perangkat komputer untuk dapat melakukan pertukaran data serta meneruskan data ke berbagai perangkat. Satu *Switch* dapat menghubungkan sejumlah perangkat sampai 48 tergantung banyaknya *port* LAN pada *switch*. Pada *management* *bandwidth* dan keamanan jaringan, *hardware* yang di gunakan berupa *Router Board* dari MikroTik.

Mikrotik adalah salah satu vendor baik *hardware* atau *software* yang menyediakan fasilitas untuk membuat router. Salah satunya Mikrotik RouterOS, yaitu OS yang khusus di gunakan untuk jaringan. Fungsi dari MikroTik adalah sebagai *management bandwidth,routing* dan sebagai *firewall*.

Dalam jaringan sering terjadinya pertukaran informasi data antar jaringan lokal maupun ke jaringan internet, namun dalam proses pertukaran data jalam jaringan lokal ataupun jaringan internet sering terjadi serangan dalam jaringan seperti percobaan masuk kerouter atau server, dan pencurian data komputer yang terhubung dalam jaringan. Selain itu, dalam jaringan dapat terjadi internet terputus ketika koneksi terputus dan jika kita menggunakan 2 ISP, kita perlu mengganti kabel secara manual. Untuk mengatasi masalah tersebut, dapat dilakukan pengaturan *backup link* dengan *automatic failover*, ketika isp utama terputus maka isp backup otomatis aktif.

*Firewall* didefinisikan sebagai sebuah komponen atau kumpulan komponen yang membatasi akses antara sebuah jaringan yang diproteksi dan internet, atau antara kumpulan-kumpulan jaringan lainnya *Firewall* merupakan solusi untuk mengatasi keamanan di dalam dunia internet baik itu keamanan komputer maupun keamanan jaringan yang banyak dipenuhi dengan berbagai ancaman baik dari dalam maupun dari luar. Dengan suatu konfigurasi yang tepat pada *firewall* maka kemungkinan untuk mengamankan suatu data atau komputer pada jaringan menjadi jauh lebih aman. (Busten, 2009)

Berdasarkan penelitian terdahulu Mohammad Badrul (2019) dan Akmaludin (2019), menyatakan bahwa Untuk mengatasi putusnya koneksi, diperlukannya suatu koneksi alternatif apabila terjadinya putus koneksi pada koneksi utama, dan koneksi alternatif (*backup connection*) akan menjalankan fungsinya dengan baik menggantikan koneksi utama secara otomatis, sehingga tujuan bisnis perusahaan akan tetap berjalan dengan baik. Capaian dari penelitian terdahulu, dilakukan implementasi automatic failover sehingga apabila terjadi putus koneksi pada koneksi utama, maka koneksi alternatif akan berjalan. Dalam penelitian terdahulu, tidak adanya recursive gateway sehingga automatic failover hanya bekerja jika koneksi dari router kemodem isp terputus dan tidak adanya firewall filtering yang dapat menyebabkan user yang terhubung kejaringan dapat mengakses router. Oleh sebab itu, untuk memaksimalkan akses internet agar tidak terputus di perlukan automatic failover dengan rekursif gateway dan keamanan jaringan menggunakan metode *firewall filtering*. Dengan adanya *automatic failover* dengan *recursive gateway* dan *firewall filtering* diharapkan semua komputer dapat menggunakan internet dengan lancar dan stabil serta terhindar dari serangan-serangan yang berasal dari dalam jaringan ataupun luar jaringan.

Sebagai solusi untuk mengatasi permasalahan yang terjadi perlu adanya optimalisasi jaringan menggunakan *automatic failover* dengan *recursive gateway* dan keamanan jaringan menggunakan menggunakan metode *firewall filtering* pada mikrotik.

Berdasarkan latar belakang masalah tersebut, maka tugas akhir ini berjudul “**PERANCANGAN DAN IMPLEMENTASI AUTOMATIC FAILOVER DAN METODE FIREWALL FILTERING PADA KEAMANAN JARINGAN BERBASIS MIKROTIK”**.

## 1.2 Identifikasi Masalah

Berdasarkan uraian singkat diatas dapat di Identifikasi beberapa masalah yang timbul yaitu :

1. Tidak adanya *recuvrise gateway* pada *automatic failover*, sehingga tidak adanya pengecekan ping ke internet yang menyebabkan *automatic failover* hanya bekerja saat koneksi mikrotik ke router terputus.
2. Tidak adanya *firewall filtering* menyebabkan *user* yang terhubung dalam jaringan bisa mengakses ke*router* dan *device* yang terhubung dalam jaringan.
3. Tidak adanya notifikasi untuk *admin* jika terdapat *user* yang mencurigakan yang mengakses jaringan.

## 1.3 Rumusan Masalah

Adapun rumusan masalah yang dapat dirumuskan berdasarkan permasalahan yang ada, yaitu :

1. Bagaimana optimalisasi jaringan menggunakan automatic *failover* dengan *recursive gateway* agar ketika *link* ISP utama terputus dan *link* ISP *backup* berjalan?
2. Bagaimana cara meningkatkan keamanan jaringan agar *user* yang terhubung dalam jaringan tidak dapat mengakses *router* dan *device* lain yang terhubung dalam jaringan?
3. Bagaimana membuat notifikasi untuk admin agar jika terdapat *user* yang mengakses *router* langsung dapat diketahui oleh *admin*?

## 1.4 Batasan Masalah

Untuk menghindari pembahasan menjadi terlalu luas, maka penulis perlu membatasinya. Adapun batasan masalah, yaitu:

* + - 1. Perangkat keras yang digunakan berupa router jenis Mikrotik dengan seri tipe RB 3011UiAS-RM yang memiliki 10 port Gigabit Lan, 1 SFP, dan panel LCD.
      2. Perpindahan ISP utama ke ISP *backup* menggunakan Automatic Failover dengan recursive gateway.
      3. *Firewall Filtering* untuk keamanan jaringan dengan pembatasan IP untuk mengakses jaringan.
      4. Notifikasi untuk *admin* menggunakan BOT Telegram jika ada *user* yang mencurigakan dalam mengakses jaringan.

## 1.5 Tujuan dan Manfaat Penelitian

Dalam tugas akhir ini penulis mempunyai tujuan-tujuan, yaitu:

* + - 1. Membuat rancangan topologi jaringan untuk implementasi *automatic failover*.
      2. Melakukan *automatic failover* ketika link ISP utama terputus, tidak perlu mengganti secara manual.
      3. Melakukan *recursive gateway* untuk pengecekan ping pada link ISP utama dan link ISP backup.
      4. Memblokir *user* yang terhubung dalam jaringan menggunakan *firewall filtering* agar tidak dapat mengakses *router* dan *device* yang terhubung dalam jaringan.

## 1.6 Metodologi Penelitian

Untuk mendapatkan hasil yang optimal, pada penelitian ini di gunakan metodologi sebagai berikut :

Studi Literatur

Studi literatur dilakukan dengan mencari dan mempelajari jurnal, artikel ilmiah dan sumber lainnya yang berkaitan dengan Implementasi Backup Link dengan *Automatic Failover* dan Metode *Firewall Filtering* Pada Keamnan Jaringan Berbasis Mikrotik

Analisis

Proses analisis di perlukan untuk mengidentifikasi permasalahan yang ada dan cara penyelesaiannya. Selain itu tahap analisis ini juga di perlukan untuk mengetahui kebutuhan perangkat keras dan perangkat lunak untuk merancang dan mengimplementasikan Backup Link dengan *Automatic Failover* dan Metode *Firewall Filtering* Pada Keamnan Jaringan Berbasis.

Perancangan

Setelah mengumpulkan data yang di perlukan dan melakukan analisis terhadap data yang sudah terkumpul, tahap selanjutnya ialah dengan melakukan proses perancangan. Proses perancangan ini meliputi perancangan topologi jaringan serta alur kerja yang akan di gunakan untuk Implementasi *Automatic Failover* dan Keamanan jaringan.

Implementasi

Tahap selanjutnya yaitu melakukan implementasi berdasarkan perancangan yang telah dilakukan. Proses implementasi ini di lakukan dengan melakukan konfigurasi backup link menggunakan *automatic failover* dan *firewall filetering* pada Mikrotik Router.

Uji Coba

Pada tahap uji coba ini di lakukan pengujian *Automatic Failover* dengan *Recursive Gateway* dengan memutus masing-masing jaringan dan melihat jalur koneksi yang dilewati menggunakan *Tracert*. Pada keamanan jaringan dilakukan ujicoba memasuki mikrotik server, yang bisa mengakses hanya ip admin.

## 1.7 Sistematika Penulisan

Agar setiap pembahasan mudah dimengerti,maka penulis menyusun sistematika laporan kerja praktek ini sebagai berikut

**BAB I PENDAHULUAN**

Bab ini membahas secara singkat terkait latar belakang, identifikasi masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metodologi penelitian, dan sistematika penulisan skripsi.

**BAB II TINJAUAN PUSTAKA**

Menjelaskan tentang tinjauan pustaka yang mendukung pemahaman penulis untuk melaksanakan penelitian yang berkaitan dengan penerapan *Backup Link* dengan *Automatic failover* dan metode *firewall filtering* pada keamanan jaringan berbasis mikrotik.

**BAB III METODOLOGI PENELITIAN**

Menjelaskan metodologi penelitian, tahapan penelitian *Automatic failover* dan metode *firewall filtering* pada keamanan jaringan berbasis mikrotik

**BAB IV HASIL DAN PEMBAHASAN**

Dalam bab ini menjelaskan tentang implementasi *bakup link* dengan *automatic failover* dan metode *firewall filtering* pada kemanan jaringan berbasis mikrotik.

**BAB V PENUTUP**

Dalam bab ini membahas terkait kesimpulan yang didapat penulis dari hasil analisis penelitian yang telah dilakukan dan saran untuk keperluan penelitian selanjutnya

# **BAB II**

# **TINJAUAN PUSTAKA**

## 2.1 Jaringan

Jaringan Komputer adalah sekumpulan komputer individu yang dihubungkan satu dengan yang lainnya menggunkan *Transmission Control Protocol* atau *Internet Protocol* (TCP/IP). Jaringan menggunakan media transmisi maupun media komunikasi lainnya, sehingga dapat saling berbagi data, informasi, program, dan sumber daya (*resource*), menggunakan bersama perangkat keras seperti harddisk, printer, pemindai dan lain sebagainya.Agar dapat mencapai tujuan yang sama, setiap bagian dari jaringan komputer meminta dan memberikan layanan (*service*). Pihak yang menerima layanan disebut klien (*client*) dan yang memberi layanan disebut *server*. Arsitektur ini disebut dengan sistem *client-server*, dan digunakan pada hampir seluruh aplikasi jaringan komputer. (Mohammad, 2019)

### 2.1.1 Klasifikasi Jaringan Komputer

1. LAN

LAN adalah jaringan komputer yang menjangkau area terbatas, seperti suatu kantor, gedung, laboratorium ataupun satu rumah dalam keluarga (Yuliandoko, 2018). LAN sekarang lebih banyak menggunakan teknologi berdasar IEEE 802.3 Ethernet switch, atau dengan Wi-Fi (Sukaridhoto, 2014). Kebanyakan berjalan pada kecepatan 10, 100, atau 1000 Mbps. Perbedaan yang mencolok antara Local Area Network (LAN) dengan Wide Area Network (WAN) adalah menggunakan data lebih banyak, hanya untuk daerah yang kecil, dan tidak memerlukan sewa jaringan. Walaupun sekarang ethernet switch yang paling banyak digunakan pada layer fisik dengan menggunakan TCP/IP sebagai protokol, setidaknya masih banyak perangkat lainnya yang dapat digunakan untuk membangun LAN. LAN dapat dihubungkan dengan LAN yang lain menggunakan router dan leased line untuk membentuk WAN. Selain itu dapat terkoneksi ke internet dan bisa terhubung dengan LAN yang lain dengan menggunakan tunnel dan teknologi VPN.

1. Metropolitan Area Network (MAN)

Metropolitan Area Network (MAN) adalah sebuah jaringan menggunakan teknologi yang sama dengan LAN, hanya ukuranya bisannya lebih luas daripada LAN, MAN dapat mencakup kantor-kantor, perusahaan yang letaknya berdekatan atau antar sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel. (Sopandi, 2010)

1. Wide Area Network (WAN)

Wide Area Network (WAN) jangkauannya mencakup daerah geografis yang lebih luas, seringkali mencakup sebuah negara bahkan benua, WAN terdiri dari kumpulan LAN dan MAN dan mesin-mesin yang bertujuan untuk menjalankan program aplikasi pemakai (Sopandi, 2010).

Pada sebagian besar WAN, jaringan terdiri dari sejumlah kabel atau saluran telepon yang menghubungkan sepasang router. Bila dua router yang tidak mengandung kabel yang sama akan melakukan komunikasi secara tak lagsung melalui router lainnya. Ketika sebuah paket dikirimkan dari sebuah router ke router lainnya melalui router perantara atau lebih, maka paket akan diterima router dalam keadaan lengkap, disimpan sampai saluran output menjadi bebas, kemudian diteruskan.

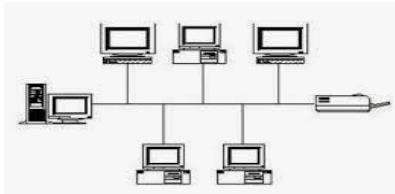
## 2.2 Topologi Jaringan

Menurut Madcom dalam Armanto menyatakan bahwa topologi jaringan adalah suatu bentuk pola penggambaran dari komponen-komponen jaringan yang saling terhubung seperti komputer server, komputer *client*/*workstation*, *hub*/*switch*, penggunaan kabel serta komponen jaringan lainnya (Armanto, 2017). Topologi jaringan diterapkan guna mempermudah *maintanance* komponenkomponen yang terlibat. Selain itu dengan diterapkannya suatu topologi, pengembangan jaringan komputer akan lebih mudah dilakukan. Jenis-jenis topologi jaringan di antaranya :

1. Topologi *Bus*
2. Topologi *Ring*
3. Topologi *Mesh*
4. Topologi *Tree*
5. Topologi *Star*

### 2.2.1. Topologi Bus

Topologi Bus adalah suatu topologi yang memiliki satu kabel *coaxsial* utama yang kedua ujungnya diakhiri dengan terminator (Haerudin, Aksara, & Yamin, 2017). Untuk terhubung dengan node, kabel utama tersebut disambungkan menggunakan *T-Connector* dan konektor BNC. Adapun contoh dari topologi bus tertera pada gambar 2.4.

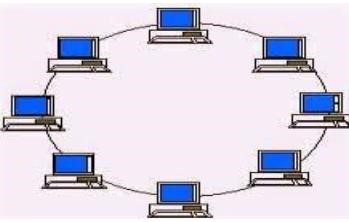


Gambar 2. 1 Topologi Bus. (Haerudin et al., 2017)

Gambar 2.1 di atas memperlihatkan contoh dari topologi bus. Kelebihan dari topologi bus yaitu pada topologi ini tidak diperlukan banyak kabel sehingga menghemat biaya instalasi. Sedangkan kekurangan dari topologi bus yaitu apabila terjadi gangguan terhadap satu komputer akan mengganggu jaringan komputer lain.

### 2.2.2. Topologi Ring

Topologi ring merupakan suatu topologi yang menghubungkan satu komputer dengan komputer lain dan seterusnya hingga kembali ke komputer pertama hingga membentuk lingkaran. Pada topologi ini setiap perangkat akan terhubung secara langsung dengan dua perangkat lain sehingga setiap node akan menggunakan 2 kabel. (Haerudin et al., 2017)

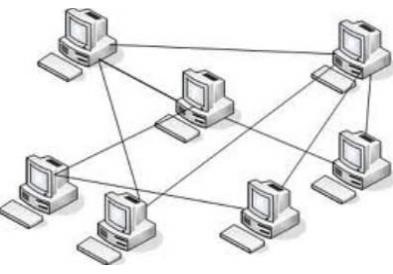


Gambar 2. 2 Contoh Topologi Ring. (Haerudin et al., 2017)

Gambar 2.2 di atas memperlihatkan contoh dari topologi ring. Keunggulan yang miliki topologi ring adalah kemudahan dalam melakukan instalasi jaringan tersebut dan penggunaan kabel yang relatif sedikit. Sedangkan kekurangan pada topologi ini yaitu apabila terjadi kerusakan pada salah satu komputer ataupun kabel, akan mengganggu pengiriman data. (Haerudin et al., 2017)

### 2.2.3. Topologi Mesh

Topologi mesh merupakan suatu jenis topologi yang menghubungkan setiap perangkat pada suatu jaringan komputer secara penuh. Dengan diterapkannya topologi mesh, kerusakan pada suatu perangkat tidak akan mempengaruhi perangkat lain atau jaringan secara keseluruhan.

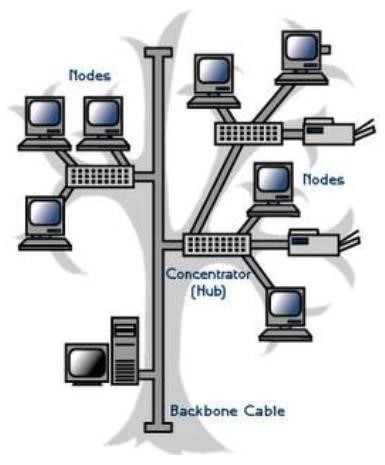


Gambar 2. 3 Contoh Topologi Mesh. (Haerudin et al., 2017)

Gambar 2.3 di atas memperlihatkan contoh dari topologi mesh. Kelebihan dari topologi mesh yaitu pada topologi ini kerusakan pada salah satu komputer tidak akan mempengaruhi komputer lain atau jaringan secara keseluruhan. Sedangkan kekurangan pada topologi mesh yaitu topologi ini membutuhkan banyak sekali kabel sehingga biaya yang diperlukan penerapan topologi ini cukup banyak. Selain itu proses instalasi pada topologi mesh ini sangat rumit. (Haerudin et al., 2017)

### 2.2.4. Topologi Tree

Topologi tree merupakan suatu jenis topologi yang terdiri dari topologi star yang terhubung dengan topologi bus, sehingga suatu topologi star akan terhubung dengan topologi star lainnya melalui topologi bus.

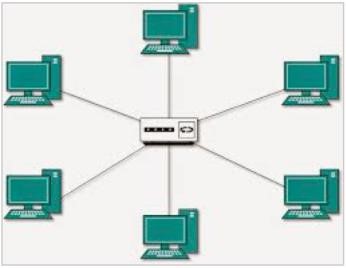


Gambar 2. 4 Contoh Topologi Tree. (Haerudin et al., 2017)

Gambar 2.4 di atas memperlihatkan contoh dari topologi tree. Kelebihan dari topologi tree yakni topologi tree sangat mudah untuk dikembangkan. Sedangkan kekurangan dari topologi tree yakni topologi ini memerlukan kabel yang cukup banyak sehingga memakan banyak biaya. (Haerudin et al., 2017)

### 2.2.5. Topologi Star

Topologi Star merupakan topologi yang paling banyak diterapkan dalam pembentukan jaringan komputer. Topologi *star* merupakan topologi yang menghubungkan semua komputer dengan konsentrator.Konsentrator pada topologi *star* dapat berupa *hub*, *switch* ataupun *router*. (Armanto, 2017)



Gambar 2. 5 Contoh Topologi Star. (Simanullang, 2018)

Gambar 2.5 memperlihatkan contoh dari desain topologi *star*. Dengan terhubungnya setiap komputer dengan node pusat / konsentrator, maka setiap pengiriman data akan melalui konsentrator tersebut terlebih dahulu. Kemudian data tersebut akan dikirimkan secara langsung oleh konsentrator ke node tujuan.

Adapun kelebihan topologi *star* antara lain :

1. Identifikasi komputer yang mengalami gangguan sangat mudah dilakukan.
2. Penambahan atau pengurangan komputer pada topologi ini sangat mudah dilakukan tanpa harus mengganggu komputer lain yang telah terhubung.
3. Keamanan suatu data yang ditransmisikan lebih tinggi.

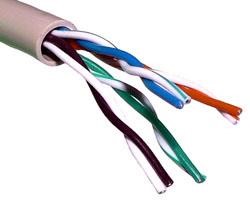
Sedangkan kekurangan dari topologi star yakni topologi ini sangat bergantung pada central node. Jika central node mengalami gangguan atau kerusakan, maka seluruh jaringan komputer pada setiap *device* yang terhubung akan mengalami gangguan. (Simanullang, 2018)

## 2.3. Media Transmisi

Pada jaringan komputer, terdapat dua jenis media transmisi yakni kabel (*wired*) dan nirkabel (*wireless*). Pada perancangan jaringan komputer dengan menggunakan media transmisi kabel, jenis kabel yang sering digunakan yaitu kabel *Unshielded Twisted Pair* (UTP) dan *Shielded Twisted Pair* (STP). Kedua kabel tersebut dapat digunakan untuk menghubungkan komputer dengan perangkat jaringan lain seperti *switch*, *hub* dan *router*. (Rajagukguk, 2020)

### 2.3.1 Kabel Unshielded Twisted Pair (UTP)

Kabel *Unshielded Twisted Pair* (UTP) merupakan jenis kabel yang terdiri dari empat pasang kabel yang dipilin (*twisted*) dan tidak memiliki pelindung (*unshielded*).

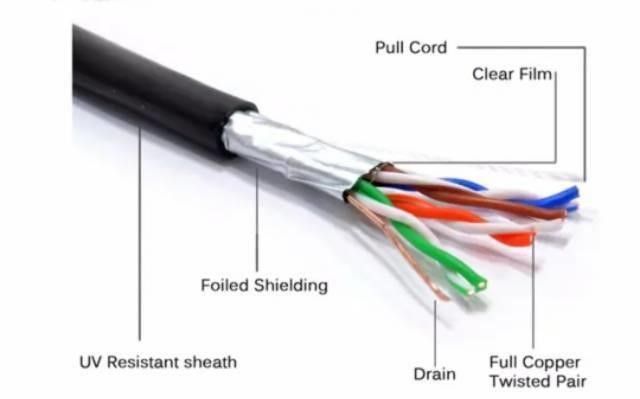


Gambar 2. 6 Kabel *Unshielded Twisted Pair* (UTP). (Rajagukguk, 2020)

Gambar 2.6 di atas merupakan contoh kabel UTP. Kabel UTP biasanya digunakan untuk menghubungkan komputer dengan perangkat jaringan lainnya seperti *switch*, *hub*, *router* dan komputer lain. Kabel UTP digunakan untuk jaringan komputer skala kecil (LAN), karena jarak jangkauannya hanya 100 meter. Kabel UTP biasanya dihubungkan ke perangkat jaringan lainnya menggunakan konektor RJ-45. (Rajagukguk, 2020)

### 2.3.2 Kabel Shielded Twisted Pair (STP)

Kabel *Shielded* *Twisted* *Pair* (STP) merupakan kabel yang memiliki fungsi yang sama dengan kabel UTP, hanya saja kabel STP memiliki pembungkus kabel ganda.



Gambar 2. 7 Kabel *Shielded Twisted Pair.* (Kurniawan, 2018)

Gambar 2.7 di atas merupakan contoh gambar dari kabel STP. Berbeda dengan kabel UTP, kabel STP memiliki pembungkus kabel ganda sehingga lebih cocok diimplementasikan di luar gedung (*outdoor*) dalam pembangunan jaringan. Sedangkan kabel UTP biasanya digunakan untuk pembangunan jaringan dalam gedung (*indoor*). (Kurniawan, 2018)

## 2.4 Router

Pada jaringan komputer, perangkat keras yang memfasilitasi transmisi paket data adalah *router.* (Rizal, 2019)



Gambar 2. 8 *Router* (Rizal, 2019)

Gambar 2.8 di atas memperlihatkan contoh dari perangkat keras *router*. *Router* memiliki fungsi sebagai penghubung antara dua jaringan atau lebih dan meneruskan paket data dari suatu jaringan ke jaringan tujuan. (Rizal, 2019)

## 2.5 Switch

*Switch* merupakan salah satu perangkat pada jaringan komputer yang berfungsi untuk menghubungkan beberapa komponen jaringan komputer agar dapat berkomunikasi. (Desmulyati, 2020)

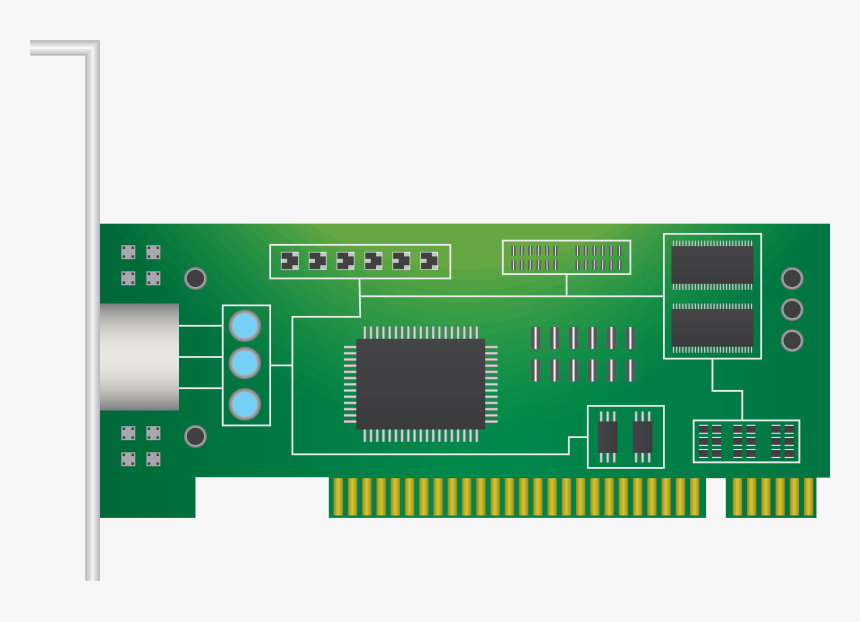


Gambar 2. 9 Switch. (Desmulyati, 2020)

Gambar 2.9 di atas merupakan contoh dari perangkat keras *switch*. Switch meneruskan paket data yang dikirim dari suatu perangkat jaringan ke perangkat lainnya. Cara kerja *switch* yakni dengan mempelajari alamat *host* tujuan, dengan demikian informasi tersebut dapat dikirim secara langsung ke *host* tujuan. (Desmulyati, 2020)

## 2.6 Network Interface Card (NIC)

*Network Interface Card* (NIC) merupakan sebuah perangkat yang menjembatani komputer agar dapat terhubung ke suatu jaringan. NIC dapat mengubungkan komputer melalui kabel (*wired*) ataupun nirkabel (*wireless*) tergantung jenis NIC yang digunakan. (Peniarsih, 2020)



Gambar 2. 10 *Network Interface Card*. (Peniarsih, 2020)

Gambar 2.10 di atas memperlihatkan contoh dari *Network Interface Card* (NIC). NIC memiliki fungsi untuk melakukan pengubahan aliran data paralel dalam bus komputer ke dalam bentuk data serial agar dapat ditransmisikan pada media jaringan. (Peniarsih, 2020)

## 2.7 IP (Internet Protocol) Address

IP (Internet *Protocol*) *Address* adalah suatu proses pemberian alamat yang berupa sederet angka yang diberikan kepada perangkat yang terhubung ke jaringan komputer seperti komputer, *router* dan perangkat lainnya (Anshori, 2019). Saat ini versi IP *address* yang digunakan adalah Ipv4, di mana pada Ipv4 terdiri dari 4 oktet (32 bit) dan setiap oktet (8 bit) dipisahkan oleh titik (dot). Angka yang Ipv4 diklasifikasikan ke dalam lima kelas. Adapun menurut Hasrul dan Lawani klasifikasi kelas pada Ipv4 sebagai berikut :

1. Kelas A, yaitu IP *address* yang terdiri dari 1 oktet pertama sebagai *network* id dan 3 oktet lainnya sebagai *host* id. *Range* oktet pertama pada IP *address* kelas A yaitu 0 sampai dengan 127.
2. Kelas B, yaitu IP *address* yang terdiri dari 2 oktet pertama sebagai *network* id dan 2 oktet lainnya sebagai *host* id. *Range* oktet pertama pada IP *address* kelas B yaitu 128 sampai dengan 191.
3. Kelas C, yaitu IP *address* yang terdiri dari 3 oktet pertama sebagai *network* id dan 1 oktet lainnya sebagai *host* id. *Range* oktet pertama pada IP *address* kelas C yaitu 192 sampai dengan 223.
4. Kelas D, yaitu IP *address* yang digunakan untuk *multicasting*. *Range* oktet pertama pada IP *address* kelas D yaitu 224 sampai dengan 239.
5. Kelas E, yaitu IP *address* yang digunakan untuk penelitian atau eksperimen. *Range* oktet pertama pada IP *address* kelas E yaitu 240 sampai dengan 255. (Lawani, 2017)

## 2.8 Modem

Modem berasal dari singkatan Modulator Demodulator. Modulator merupakan bagian yang mengubah sinyal informasi kedalam sinyal pembawa (carrier) dan siap untuk dikirimkan, sedangkan Demodulator adalah bagian yang memisahkan sinyal informasi (yang berisi data atau pesan) dari sinyal pembawa yang diterima sehingga informasi tersebut dapat diterima dengan baik. Modem merupakan penggabungan kedua-duanya, artinya modem adalah alat komunikasi dua arah. (Saputro, 2015)

## 2.9 Mikrotik

Mikrotik adalah sistem operasi yang berbasis Linux yang difungsikan sebagai router dalam jaringan. Untuk instalasi mikrotik tidak dibutuhkan perangkat lunak tambahan atau komponen tambahan lain. Mikrotik di desain mudah digunakan untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga yang kompleks sekalipun. (Riadi, 2010)

Mikrotik merupakan sistem operasi linux base yang dirancang secara khusus untuk keperluan networking. Didesain untuk memberikan kemudahan bagi penggunanya. Mikrotik dapat dilihat seperti Winbox. Winbox merupakan 15 perangkat lunak untuk me-remote mikrotik dalam GUI (Graphic User Interface) sehingga user dengan mudah dapat mengakses dan mengkonfigurasi router sesuai kebutuhan dengan mudah, efektif, dan efisien Selain itu instalasi dapat dilakukan pada standard PC (Personal Computer). (Sinaga, Sitompul, & Saleh, 2012)

## 2.9 Firewall Filter Rules

Filter filter rules merupakan salah satu fitur yang terdapat di MikroTik Router OS yang berfungsi sebagai pembatas ataupun pemberi akses paket koneksi. Di dalam filter rules terdapat fungsi DROP (menutup), ACCEPT (mengijinkan) yang digunakan sebagai pemberi akses paket koneksi baik koneksi yang diijinkan maupun paket yang tidak diperbolehkan melewati router. Seperti halnya firewall mangle di dalam filter rules terdapat fungsi seperti connection byte, content dan dst address list sebagai parameter untuk menandai paket yang akan di eksekusi. Yang menjadi perbedaan antara firewall mangle dan filter rules adalah apabila firewall mangle bertugas sebagai penanda paket yang nantinya akan di eksekusi oleh limiter (pada umumnya) sedangkan firewall filter rules bertugas sebagai pemberi akses untuk paket-paket yang diinginkan. Sebagai contoh apabila ingin dilakukan pembatasan kecepatan untuk paket tertentu maka yang bertanggung jawab adalah firewall mangle dan limiter, namun apabila ingin menutup akses ke alamat website atau IP tertentu maka ini menjadi tugas filter rules dan bias di kombinasikan dengan address list. (Utomo, 2014)

## 2.10 Address List

Address list adalah “tempat” untuk mengelompokan IP yang akan dijadikan sebuah group. Dengan menggunakan address list ini lebih memudahkan apabila ingin menggunakan beberapa IP saja dari dalam satu segmen IP. IP yang akan di daftarkan nantinya dapat secara acak, hanya saja penamaan group dari IP tersebut harus sama apabila ingin masuk dalam satu group. Fungsinya adalah apabila memerlukan pembatasan kecepatan akses secara group, dapat menggunakan fitur ini untuk melakukan pendataan IP. (Utomo, 2014)

## 2.11 Failover

*Failover* adalah sebuah teknik menambahkan koneksi di mikrotik, dimana jika salah satu koneksi internet mati (koneksi utama) maka koneksi yang satunya (koneksi cadangan) akan mem-*backup* koneksi utama. Dan pergantian koneksi dari koneksi utama ke koneksi cadangan akan berjalan secara otomatis. (Towidjojo, 2019)

## 2.12 Winbox

WinBox adalah sebuah utility yang digunakan untuk melakukan remote ke server mikrotik dalam mode GUI (Valens, 2004). Jika untuk mengkonfigurasi mikrotik dalam text mode melalui PC itu sendiri, maka untuk mode GUI yang menggunakan winbox ini dapat melakukan konfigurasi mikrotik melalui komputer client.

Winbox dibuat menggunakan win32 binary tapi dapat dijalankan pada linux, MAC OSX dengan menggunakan wine. Semua fungsi winbox di desain semirip dan sedekat mungkin dengan fungsi console. Hal ini karena menggunakan winbox dirasa lebih mudah dibandingkan melalui browser. (Pamungkas, 2016)

## 2.13 Gateway

Gateway adalah sebuah perangkat yang digunakan untuk menghubungkan satu jaringan komputer dengan satu atau lebih jaringan komputer yang menggunakan protokol komunikasi yang berbeda sehingga informasi dari satu jaringan komputer dapat diberikan kepada jaringan komputer lain yang protokolnya berbeda. (Sinaga, 2012)

## 2.14 ISP (*Internet Service Provider*)

ISP (Internet Service Provider) adalah perusahaan atau badan penyedia jasa layanan internet kepada pelanggan, ISP diidentikan dengan perusahaan jasa telekomunikasi, karena dulu ISP menawarkan produknya melalui jaringan telepon. Mereka menyediakan jasa seperti hubungan ke internet, pendaftaran nama domain, dan hosting contohnya Telkom, Indosat, dan lain sebagainya. Saat ini ISP berkembang tidak hanya dengan menggunakan jaringan telepon, tetapi juga menggunakan teknologi seperti fiber optic dan wireless. (Amin, 2015)

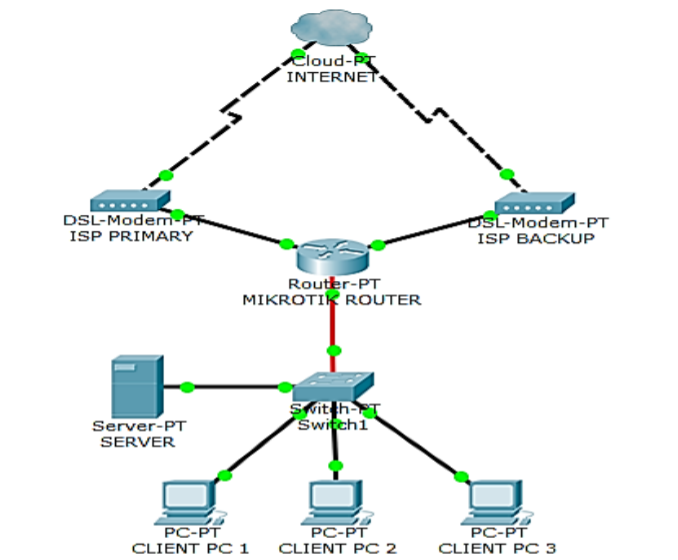
# **BAB III**

# **METODOLOGI PENELITIAN**

## Analisis Sistem Jaringan Berjalan

### Topologi Jaringan

Pada topologi jaringan ini, terdapat 2 Modem ISP, 1 Router Mikrotik RB2011UiAS-2Hnd, 3 PC dan 1 buah *switch* 16 ports. Adapun topologi jaringan komputer tersebut menggunakan topologi *star* seperti yang tertera pada gambar 3.1.



Gambar 3.1 Topologi Jaringan Berjalan

Pada skema jaringan yang berjalan saat ini menggunakan topologi star. Topologi star banyak di gunakan karena mudah untuk mendeteksi apabila ada perangkat yang terhubung dengan *switch* mengalami kerusakan. Misalkan terdapat komputer rusak, maka lampu indikator *switch* pada *port* yang terhubung akan mati.

Router MikroTik yang di gunakan pada penelitian terdahulu ini bertipe MikroTik RB-2011UiAS-RM, router tersebut memiliki 5 Port Lan dan 5 Ports Gigabit lan. *Port lan* dalam *router* ini dapat di gunakan sebagai *wan* yang berfungsi untuk dijadikan *backup link* ISP, selain itu *router* yang di gunakan *support* dengan software winbox seri terbaru yang berfungsi untuk mengatur dan konfigurasi *failover dan firewal*.

### Hardware Dalam Jaringan

Alat yang di gunakan dalam sistem berjalan ini terdiri perangkat keras dan perangkat lunak. Perangkat keras yang digunakan adalah router mikrotik RB-2100UiAS-RM, *switch*, dan 3 komputer. Berikut *hardware* yang di gunakan sebagai berikut:

**Mikrotik RB-2011UiAS-RM**

Spesifikasi *Router Server* yang terdapat dalam Topologi Jaringan ini adalah sebagai berikut.

Tabel 3.1 Spesifikasi Mikrotik RB 2011UiAS-RM

|  |  |
| --- | --- |
| Product code | RB2011UiAS-RM |
| Architecture | MIPS-BE |
| CPU | AR9344 600MHz |
| CPU core count | 1 |
| Wireless Standarts | 802.11 b/g/n |
| Dimensions | 250x250x90mm |
| RouterOS license | 5 |
| Operating System | RouterOS |
| Size of RAM | 128 MB |
| Storage size | 64 MB |
| Storage type | NAND |
| Tested ambient temperature | -30°C to 70°C |

Tabel di atas menjelaskan spesifikasi dari router yang digunakan. Berdasarkan tabel di atas dapat diketahui spesifikasi secara rinci komputer Proccessor, CPU Freq, Storage, dan Ram.

**Switch D-LINK DGS-1016C**

Spesifikasi *Switch* yang terdapat dalam Topologi Jaringan ini adalah sebagai berikut.

Tabel 3.2 Spesifikasi Switch D-Link DGS-1016C

|  |  |
| --- | --- |
| Product code | DGS-1016C |
| Switching Features | 32 Gbps switching fabric |
| Power Supply | 100 to 240V AC |
| Ports | 16 10/100/1000 Mbps LAN Ports |
| Dimensi Produk | 282.2 x 178.0 x 44.5 mm |
| Power Consumption | * 1. Watts |

### Perangkat Lunak Pendukung

Perangkat lunak yang digunakan dalam sistem jaringan berjalan adalah sebagai berikut:

1. **Winbox**

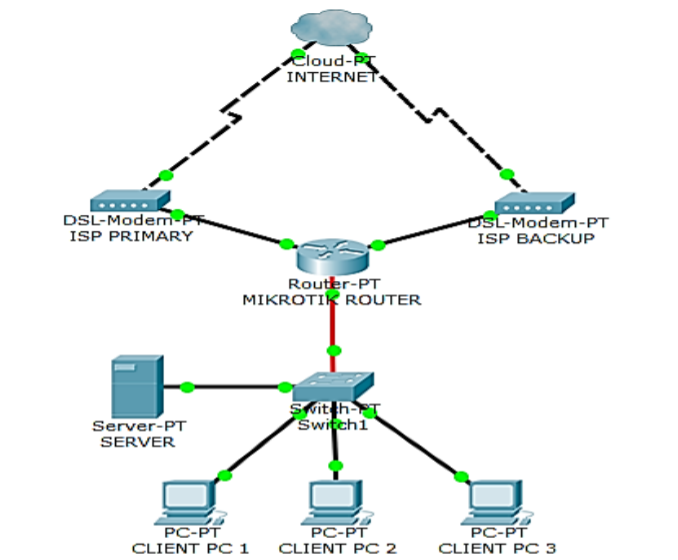
Software yang di gunakan untuk melakukan konfigurasi pada router berjenis mikrotik. Winbox dapat mengatur konfigurasi, seperti managemen bandwidth dan firewall pada router.

1. **Sistem Operasi**

Sistem operasi yang digunakan komputer klien pada sistem berjalan yaitu Windows 10.

## Anaisis Permasalahan Sistem Jaringan Berjalan

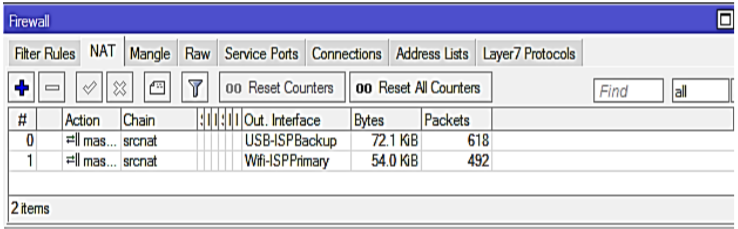
### Analisis Automatic Failover



Gambar 3.2 Topologi Star pada Automatic Failover

Permasalahan jaringan yang ada berada pada automatic failover, dimana automatic failover hanya memeriksa koneksi link anara ISP Primary ke Mikrotik router, sehingga tidak ada pengecekan jaringan ke Internet. Kedala yang dapat terjadi ketika koneksi Internet terputus namun koneksi ke modem ISP Primary tidak terputus maka automatic failover tidak berjalan.

### Analisis Firewall Filtering



Gambar 3.3 Firewall Filtering

Setelah di analisis keamanan jaringan, tidak adanya firewall filtering yang membatasi atau memblokir IP user yang terhubung kejaringan selain admin sehingga user yang terhubung dalam jaringan dapat mengakses router ataupun *device* seperti komputer yang terhubung dalam jaringan.

## Analisis Kebutuhan Jaringan

### Spesifikasi Kebutuhan Perangkat Lunak

Analisis perangkat lunak bertujuan untuk memilih secara tepat perangkat lunak apa saja yang digunakan untuk melakukan konfigurasi *automatic failover* dengan *recursive gateway* dan keamanan jaringan dengan *firewall filtering* agar dapat beroperasi dengan efektif dan efisien. Berikut keterangan perangkat lunak yang dibutuhkan dan akan digunakan untuk melakukan konfigurasi :

|  |  |  |
| --- | --- | --- |
| **No** | **Software** | **Keterangan** |
| 1. | Winbox | Software untuk melakukan remote GUI/CLI ke router mikrotik |
| 2. | Windows 11 Pro 64 bit | Sebagai Sistem Operasi |
| 3. | Command Promt | Sebagai Pengujian Jalur Internet |

### Spesifikasi Kebutuhan Perangkat Keras

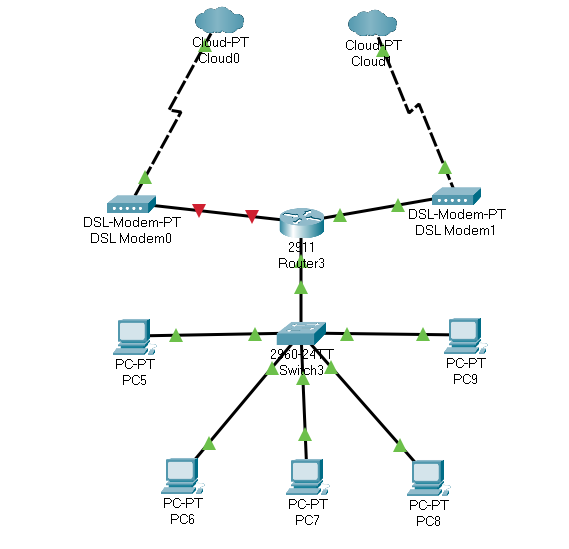
Analisis perangkat keras bertujuan untuk memilih secara tepat perangkat keras apa saja yang dibutuhkan untuk perancangan dan implementasi *automatic failover* dengan *recursive gateway*. Berikut keterangan perangkat keras yang dibutuhkan :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Perangkat Keras** | **Jumlah (Unit)** | **Spesifikasi Unit** | **Keterangan** |
| 1. | Routerboard Mikrotik | 1 | RB 3011UiAS-RM | Penghubung Antar ISP, Management |
| 2. | Laptop/PC | 1 | Asus Core i5 3,4Ghz 8GB/256GB |  |
| 3. | ISP | 2 | * Biznet Networks * Telkom Indonesia | Sebagai Sumber Internet Service Provider |
| 4. | Switch | 1 | TP Link 16 Ports Gigabit | Sebagai Switching antar perangkat |

## Sistem Jaringan Usulan

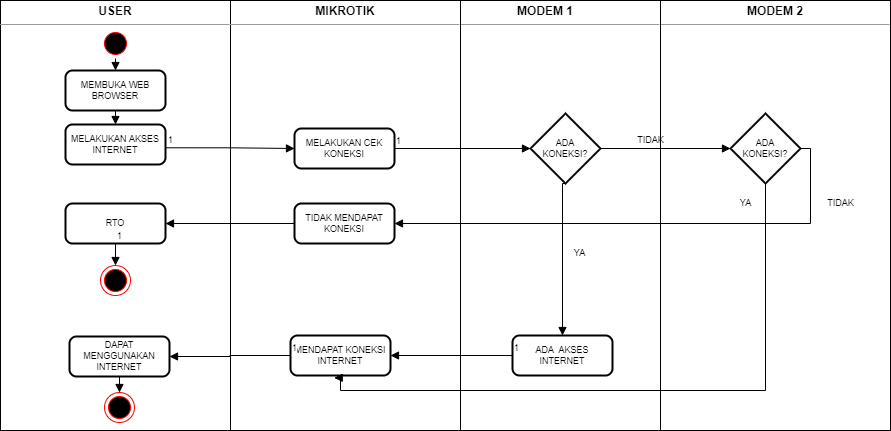
### Topologi Jaringan

Pada topologi jaringan usulan ini penulis menggambarkan dengan menggunakan perangkat lunaksimulasi jaringan *Cisco* *Packet Tracer*, penulis memberikan gambaran topologi jaringan yang akan di gunakan dalam perancangan jaringan usulan untuk implementasi *automatic failover*. Skema jaringan yang diusulkan adalah sebagai berikut:



Gambar 3.4 Topologi Jaringan Usulan

Dari Topologi Jaringan di atas menggambarkan modem yang berasal dari ISP 1 dan ISP 2 terhubung ke router menggunakan kabel LAN. Koneksi ISP 1 berasal dari Modem 0 yaitu ISP Utama, sedangkan ISP 2 berasal dari modem 1 yaitu ISP Backup. Jika ISP 1 tidak memiliki koneksi internet, maka dilanjutkan pengalihan secara otomatis ke ISP 2 sebagai *link* backup sehingga pengguna dapat menggunakan koneksi internet tanpa terputus dari ISP 2.

Selanjutnya pada gambar di bawah ini terdapat *activity diagram* usulan untuk menggambarkan bagaimana sistem saling terhubung :

Gambar 3.5 Activity Diagram Usulan

Gambar 3.5 di atas menjelaskan kerja alur sistem yang di rancang sebagai berikut.

1. Pengguna atau user menggunakan komputer dan melakukan aktivitas *browsing* menggunakan *web browser* dan melakukan akses internet.
2. Selanjutnya router mikrotik memeriksa ketersediaan akses internet pada ISP 1(Modem 1) sebagai *link* utama, Jika ISP 1 tidak memiliki koneksi internet maka akan di lanjutkan pengalihan ke ISP 2.
3. Mikrotik akan memeriksa ketersediaan akses internet pada ISP 2(Modem 2) sebagai *link backup*.
4. Jika ISP 2 memiliki koneksi internet, maka router mikrotik akan mendapat koneksi internet lalu di alirkan ke *user* agar dapat menggunakan internet.
5. Jika ISP 2 tidak memiliki koneksi internet, maka *router* mikrotik tidak mendapat koneksi internet lalu user tidak dapat mengakses internet.

### Pengalamatan IP Address

IP *address* yang akan digunakan dalam perancangan jaringan usulan adalah sebagai berikut :

Tabel 3.4 Pengalamatan IP Address

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | Perangkat | Interface | IP Address | Gateway |
| 1 | Modem 1 (Biznet) | Gigabit Ethernet | 192.168.19.1/24 | 192.168.19.1 |
| 2 | Modem 2 (Telkom) | Gigabiet | 192.168.8.1/24 | 192.168.8.1 |
| 3 | Mikrotik RB-3011UiAS-RM  Mikrotik RB-3011UiAS-RM | ISP Utama (Biznet)  ISP Backup (Telkom) | 192.168.19.12/24  192.168.8.170/24 | 192.168.19.1  192.168.8.1 |
| 4 | Mikrotik RB-3011UiAS-RM | Ethernet | 192.168.20.2-254 | 192.168.20.1 |
| 5 | LAPTOP | Ethernet | 192.168.20.254/24 | 192.168.20.1 |

Terdapat perangkat dan Interface dengan penjelasan sebagai berikut :

1. Modem 1 (Biznet) : Merupakan sumber internet ISP Utama yang dihubungkan ke WAN-1 pada mikrotik.
2. Modem 2 (Telkom) : Merupakan sumber internet ISP Backup yang dihubungkan ke WAN-2 pada mikrotik.
3. WAN 1 dan 2 pada mikrotik sebagai penerima IP DHCP dari masing-masing modem.
4. Ethernet Mikrotik : merupakan interface lokal mikrotik yang terkoneksi dengan jaringan lokal yang terhubung dengan switch.

Source code untuk pengalamatan IP Address pada mikrotik.

|  |
| --- |
| /ip address add address=192.168.19.12/24 network=192.168.19.0 interface=1.ISP-UTAMA  add address=192.168.8.170/24 network=192.168.8.0 interface=2.ISP-BACKUP  add address=192.168.20.1/24 network=192.168.20.0 interface=LAN |

1. Port WAN 1 pada mikrotik diberikan nama Interface ISP-UTAMA dengan ip address 192.168.19.12.
2. Port WAN 2 pada mikrotik diberikan nama Interface ISP-BACKUP dengan ip address 192.168.8.170.
3. Port LAN yang akan terhubung dengan switch dan komputer diberikan ip 192.168.20.1 sebagai dhcp server.

### Perancangan Automatic Failover dengan Rekursif Gateway

Berikut adalah tahapan-tahapan yang harus dilalui untuk melakukan konfigurasi load balancing pada mikrotik :

#### **Automatic Failover**

*Failover* berguna untuk menangani jika terjadi putus koneksi pada salah satu jalur ke *gateway* *modem*. Diharapkan *failover* ini akan melakukan perpindahan *gateway* secara otomatis ke *link backup*. *Automatic failover* memanfaatkan proses pemeriksaan *gateway* dengan mengirimkan ping ke modem untuk mendeteksi kegagalan sebuah jalur. Dengan cara ini maka kegagalan jalur yang disebabkan oleh gagalnya *hop* dalam proses transaksi data juga dapat terdeteksi.

#### **Recursive Gateway**

Selanjutnya *recursive gateway* akan memetakan routing atau jalur koneksi berdasarkan *routing* yang sudah dibuat pada route list. *Recursive gateway* akan memeriksa ketersediaan internet dengan mengirimkan ping atau paket icmp ke dns google melalui gateway modem ISP utama dan ISP *backup*.

#### **Firewall Filtering**

Selanjutnya *firewall filtering* berfungsi atau bekerja memblokir seluruh IP Address, terkecuali IP 192.168.20.254 sehingga hanya IP Admin tersebut yang hanya dapat mengakses mikrotik ataupun *device* lain yang terhubung dalam jaringan.

### Perancangan Notifikasi Untuk Admin

Berikut adalah tahapan-tahapan yang harus dilalui untuk membuat notfikasi ke admin pada mikrotik :

#### **Script Scheduler**

Selanjutnya *script scheduler* berfungsi untuk menjalankan *script* yang mengirimkan pesan keAdmin untuk memberi notifikasi ke admin terkait aktifitas mencurigakan dalam jaringan.

## Langkah-langkah Pengujian

Pada tahapan ini, penulis akan melakukan beberapa pengujian kinerja *automatic failover* dan kemanan jaringan dengan masing-masing cara diantaranya sebagai berikut :

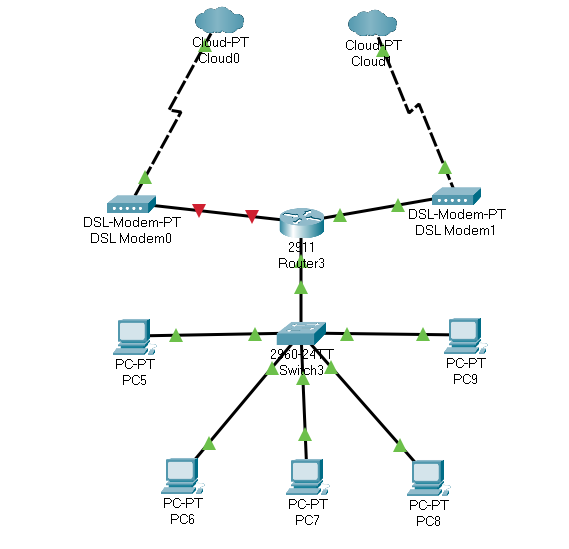
1. Ketersediaan Jaringan : Jika terdapat koneksi internet ISP Utama mati, maka *failover* akan berhenti mengirimkan *request ping* ke *gateway* modem dan mengalihkan ke ISP *Backup*. Pengujian dilakukan dengan memutus koneksi disalah satu sumber internet ISP Secara bergantian.
2. Pengecekan jalur *hops* yang dilalui data dengan menggunakan perintah *Tracert* pada CMD, dari perintah *tracert* maka didapatkan hasil hops-hops yang yang dilalui data.
3. Pada keamanan jaringan, dapat diUji dengan mencoba remote dan mengirimkan paket ping ke *gateway router* mikrotik. Pengujian dilakukan dengan memblokir akses IP terkecuali IP admin, dan penulis mencoba dimasing-masing IP.
4. Uji coba notifikasi *reminder* untuk admin dengan cara melakukan akses mikrotik dengan memasukkan *username* dan *password* dengan benar dan salah.

# **BAB IV**

# **HASIL DAN PEMBAHASAN**

## Pembangunan Infrastruktur

Hasil dari perancangan jaringan usulan yang sebelumnya telah diuraikan kemudian dilakukan pembangunan infrastrukur dan konfigurasi agar jaringan yang dirancang dapat berjalan dengan baik, yaitu dengan pembangunan infrastruktur seperti gambar 4.1.



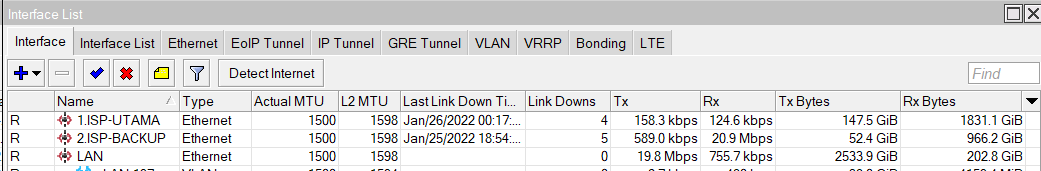
Gambar 4.1 Topologi Jaringan Yang Digunakan

Berdasarkan topologi jaringan pada gambar 4.1 yang disusun untuk menghubungkan dua sumber koneksi internet, proses yang dilakukan pertama kali adalah konfigurasi dan pengalamatan IP address pada setiap perangkat routerboard yang ada dalam jaringan.

## Konfigurasi Jaringan

### Interface

Konfigurasi penamaan interface agar memudahkan mengetahui sumber internet dan jaringan lokal untuk konfigurasi selanjutnya.Penamaan yang digunakan berupa ISP Utama, ISP *Backup*, dan LAN



Gambar 4.2 Tampilan Interface List

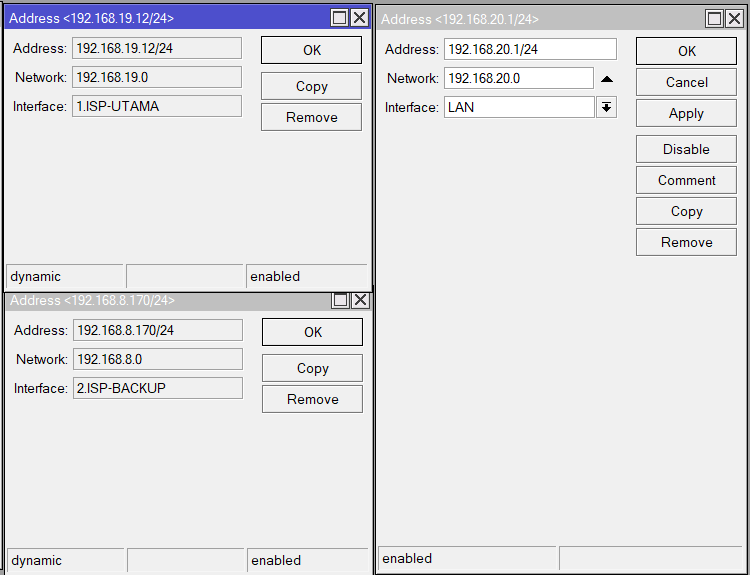
### Konfigurasi IP Address

IP Address yang digunakan dalam implementasi jaringan ini adalah IP Address kelas C karena jaringan ini tidak membutuhkan banyak IP.

IP ISP Utama > 192.168.19.12

IP ISP Backup > 192.168.8.170

IP LAN > 192.168.20.1 (IP Local)

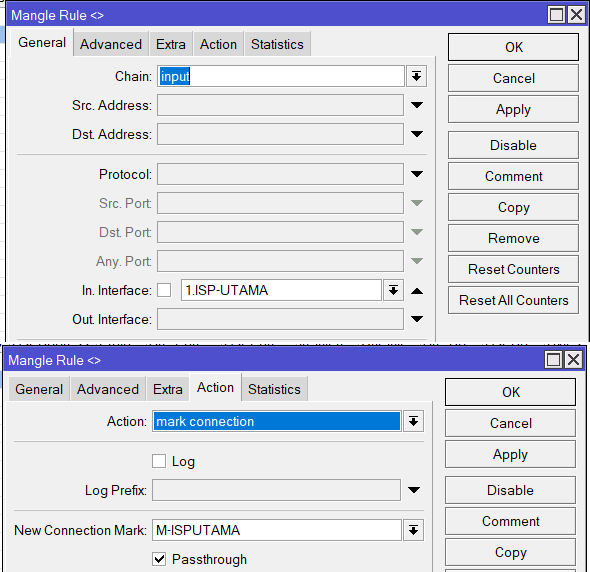


Gambar 4.3 IP Address

### Konfigurasi Automatic Failover

Berikut merupakan tahapan konfigurasi mangle *Automatic Failover* untuk menandakan routing dan paket yang melewati masing-masing *gateway* modem ISP, berikut konfigurasinya :

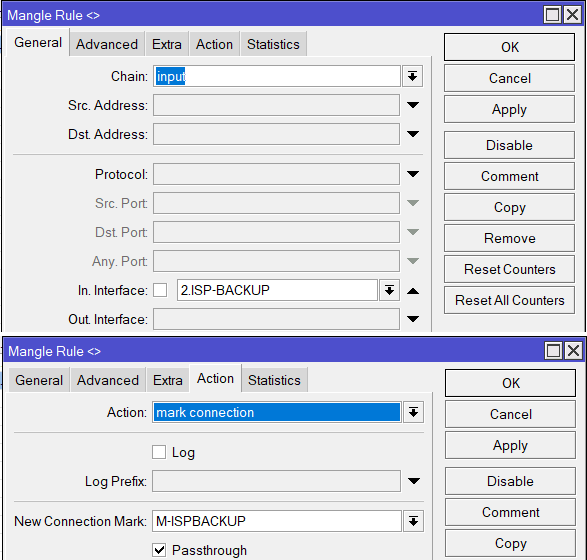
1. Konfigurasi Input ISP 1



Gambar 4.4 Konfigurasi Mangle Input ISP 1

Pada gambar 4.4 adalah konfigurasi input untuk menandakan koneksi dari ISP 1.

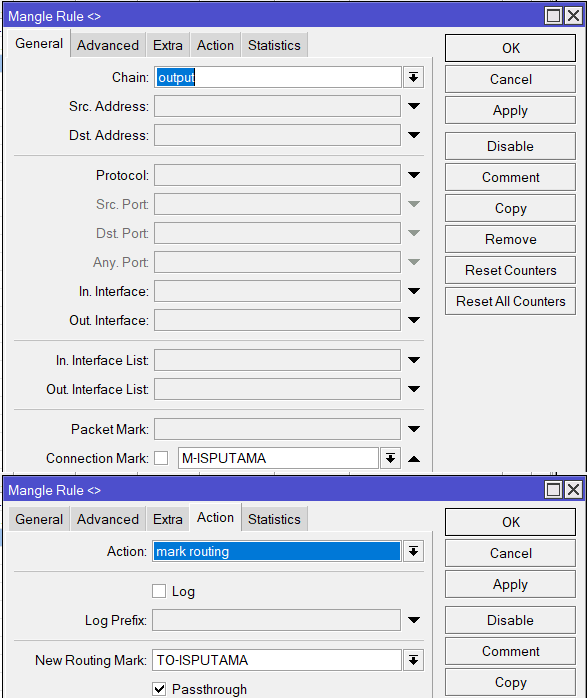
1. Konfigurasi Input ISP 2



Gambar 4.5 Konfigurasi Mangle Input ISP 2

Pada gambar 4.5 adalah konfigurasi *input* untuk menandakan koneksi dari ISP 2.

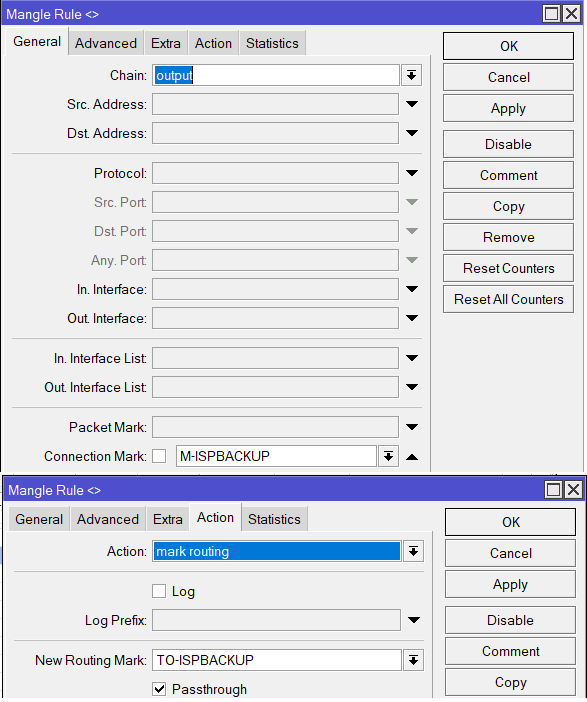
1. Konfigurasi Output ISP 1



Gambar 4.6 Konfigurasi Mangle Output ISP 1

Pada gambar 4.6 adalah konfigurasi *output* untuk menandakan *routing output* dari ISP 1.

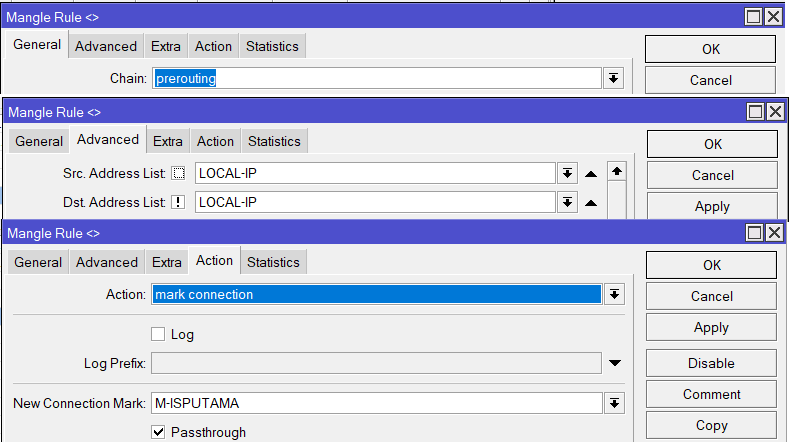
1. Konfigurasi Output ISP 2



Gambar 4.7 Konfigurasi Mangle Output ISP 1

Pada gambar 4.7 adalah konfigurasi output untuk menandakan *routing output* dari ISP 2.

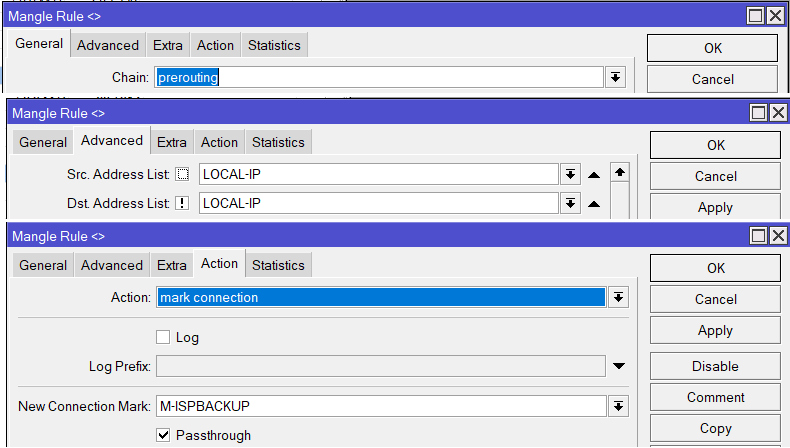
1. Konfigurasi Mangle prerouting Local IP



Gambar 4.8 Konfigurasi Mangle prerouting

Pada gambar 4.8 adalah konfigurasi mangle menandakan koneksi dari koneksi lokal sebelum dirouting, jika masuk melalui ISP 1 maka keluar dari ISP 1.

1. Konfigurasi Mangle prerouting local ip



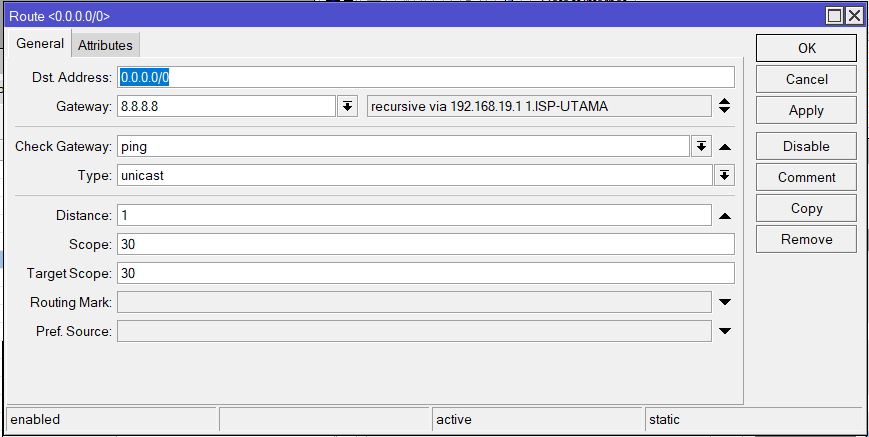
Gambar 4.9 Konfigurasi Mangle prerouting

Pada gambar 4.9 adalah konfigurasi mangle menandakan koneksi dari koneksi lokal sebelum dirouting, jika masuk melalui isp 2 maka keluar dari isp 2.

### Konfigurasi Recursive Gateway

Berikut merupakan tahapan konfigurasi *recursive gateway* untuk pengecekan ketersediaan internet atau koneksi melalui *gateway* ping atau internet, berikut konfigurasinya :

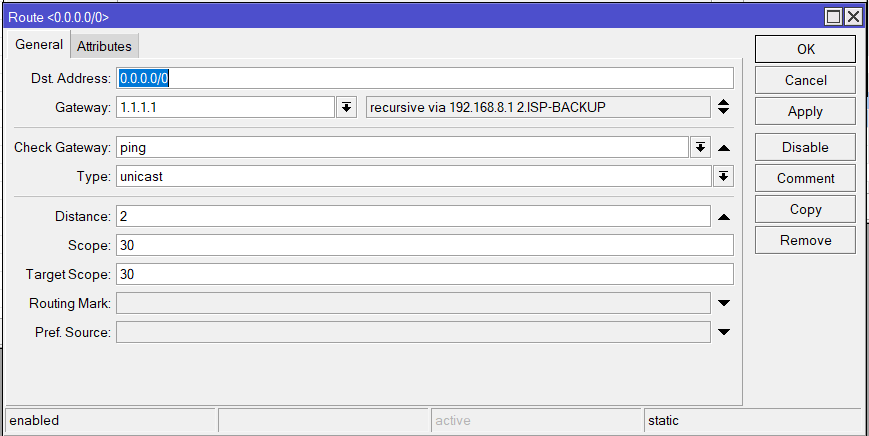
Recursive ISP Utama



Gambar 4.10 Konfigurasi Recursive ISP Utama

Pada gambar 4.10 adalah konfigurasi *recursive* untuk melakukan pengecekan koneksi internet ke dns 8.8.8.8 melalui *gateway* ISP Utama.

* 1. Recursive ISP Backup

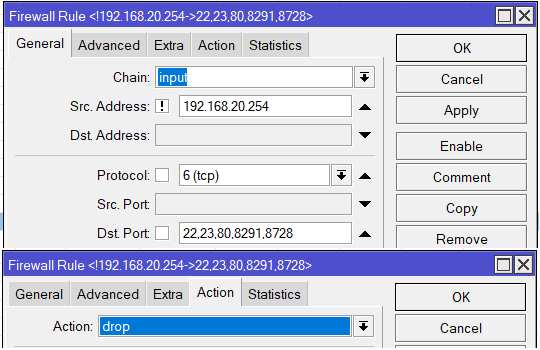


Gambar 4.11 Konfigurasi Recursive ISP Backup

Pada gambar 4.11 adalah konfigurasi *recursive* untuk melakukan pengecekan koneksi internet ke dns 1.1.1.1 melalui gateway ISP *Backup*, jika ISP Utama mati.

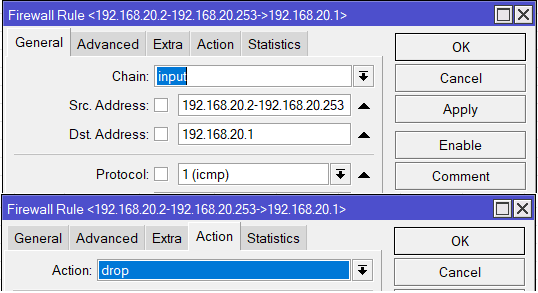
### Konfigurasi Keamanan Jaringan

Berikut merupakan tahapan konfigurasi kemanan jaringan, agar user atau pengguna yang tidak dinginkan tidak dapat mengakses router ataupun *device* yang terhubung dalam jaringan, berikut konfigurasinya :



Gambar 4.12 Konfigurasi Blokir Akses

Pada gambar 4.12 adalah konfigurasi IP *whitelist*, IP yang terdaftar dapat mengakses router atau device yang terhubung dalam jaringan sesuai *port* yang digunakan

.

Gambar 4.13 Konfigurasi Blokir Ping

Pada gambar 4.13 adalah konfigurasi IP *blacklist*, sehingga *user* selain IP admin tidak dapat melakukan pengecekan ping atau ping *flood ke gateway* router.

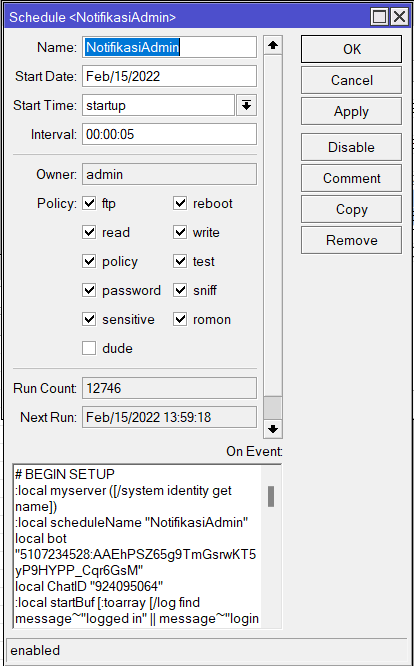
### Konfigurasi Notifikasi Admin

Berikut merupakan tahapan pembuatan notifikasi untuk admin agar admin mendapatkan *reminder* jika terdapat aktifitas yang mencuriakan, berikut tahapannya :

Pembuatan Bot Telegram

Pada Telegram, tambahkan pertemanan BotFather lalu buat bot serta dapatkan token dari bot yang dibuat. Lalu tambahkan get\_id\_bot untuk mendapatkan chatID.

Konfigurasi Notifikasi Admin



Gambar 4.14 Konfigurasi Notifikasi Admin

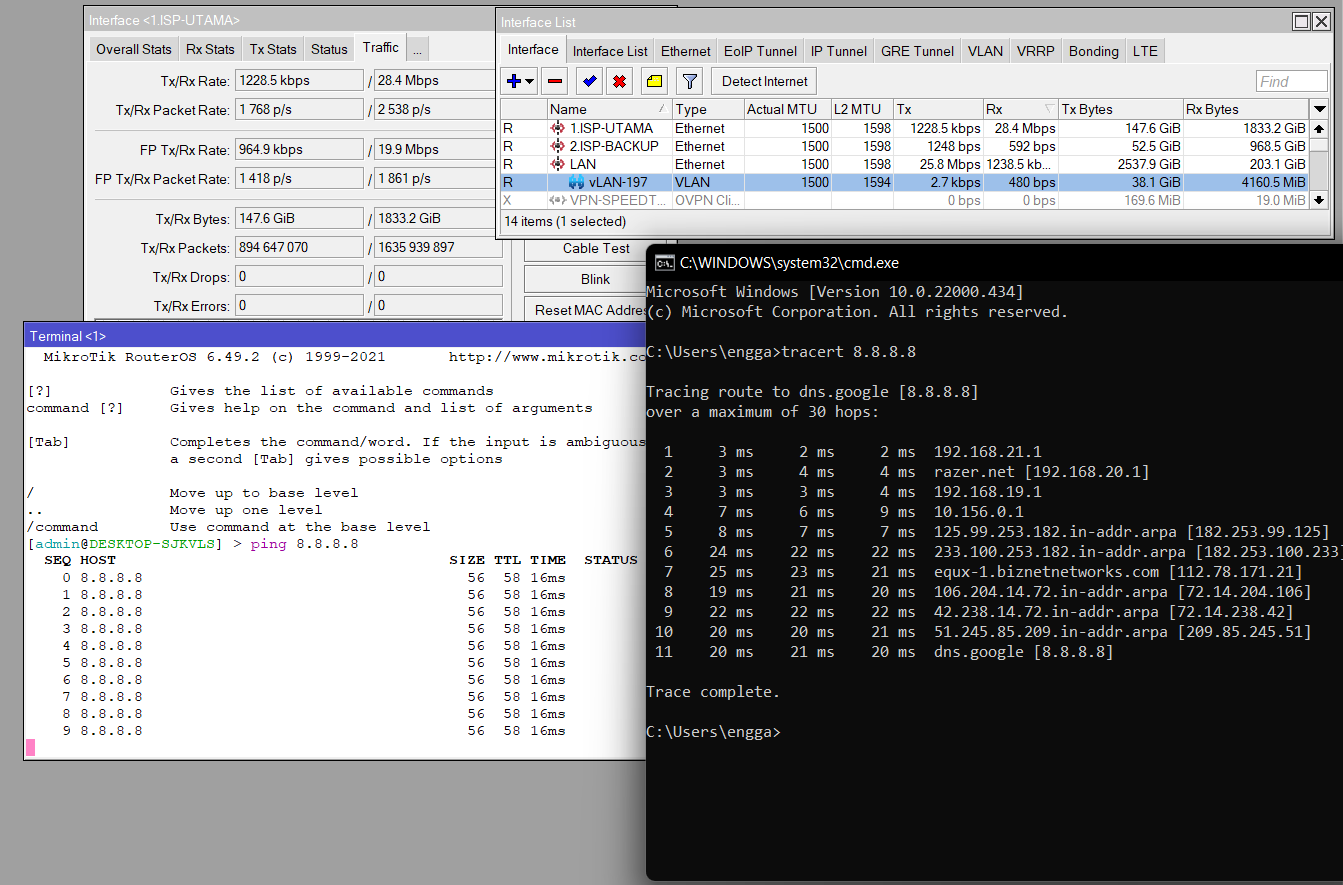
Pada gambar 4.14 adalah scheduler untuk notifikasi admin, sehingga setiap 5 detik sekali scheduler melakukan pengecekan aktifitas log, jika terdapat aktifitas log yang mencurigakan maka router akan mengirimkan Notifikasi ke Admin melalui bot telegram dengan API yang sudah dibuat.

## Pengujian dan Hasil

Setelah melakukan tahap perancangan dan implementasi, maka tahap selanjutnya adalah melakukan pengujian akhir dengan mensimulasikan untuk memberikan pemecahan masalah pada penelitian terdahulu menggunakan jaringan lokal sesuai dengan perancangan yang telah dibuat.

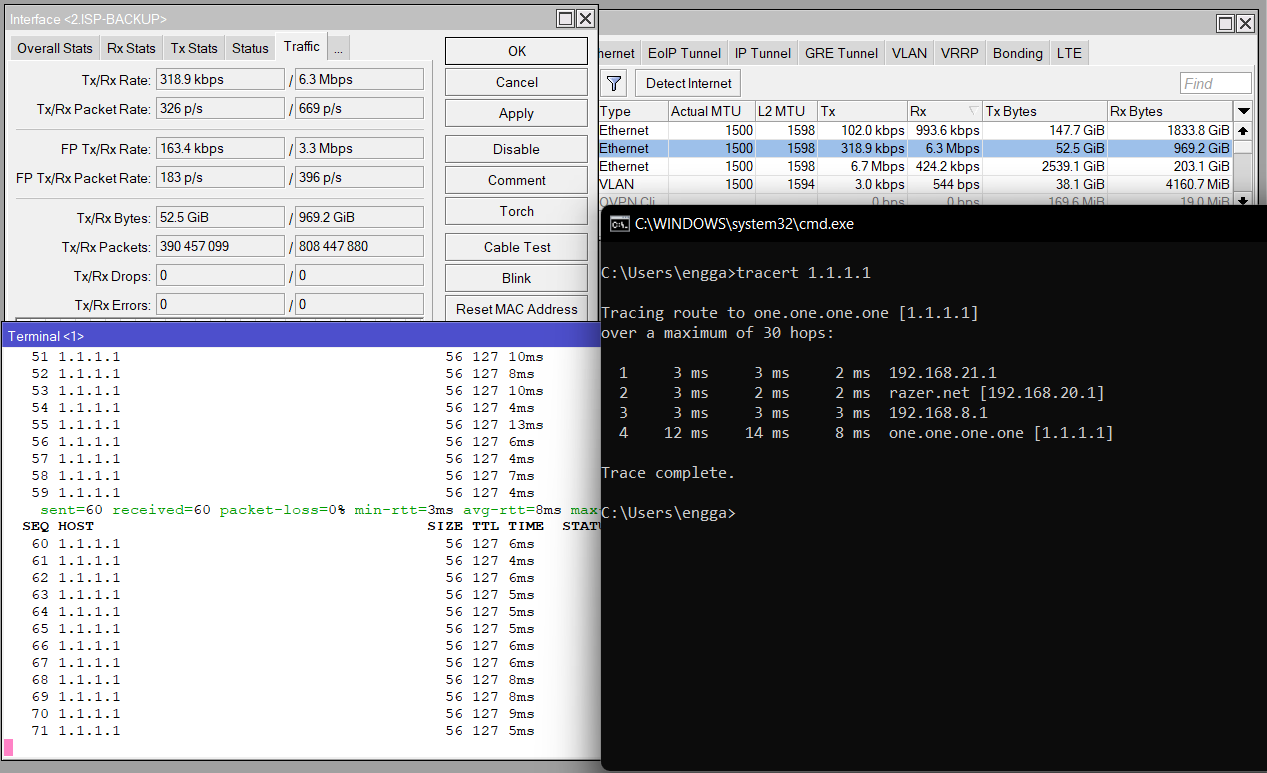
### Pengujian Automatic Failover dengan Recursive Gateway

Tahapan pengujian masih berjalan menggunakan ISP Utama, terlihat pada Terminal mikrotik jika ISP Utama selalu memberikan koneksi dan dilakukan pengujian Jalur yang digunakan dapat terlihat pada terminal CMD menggunakan traceroute menghasilkan jalur yang dilewati Komputer melalui router (192.168.20.21), lalu mikrotik (192.168.20.1), selanjutnya modem ISP Utama (192.168.19.1)



Gambar 4.15 Pengujian Saat ISP Utama Tidak Mengalami Gangguan

Tahapan pengujian jika ISP Utama sedang mengalami gangguan, bisa terlihat terlihat Interface ISP *Backup* langsung berjalan sebagai perannya ISP *Backup*. Dan dilakukan test koneksi menggunakan traceroute, jalur yang digunakan dapat terlihat pada terminal CMD menggunakan tracert menghasilkan jalur yang dilewati Komputer melalui router (192.168.20.21), lalu mikrotik (192.168.20.1), selanjutnya modem ISP *Backup* (192.168.8.1), dan berakhir di dns 1.1.1.1



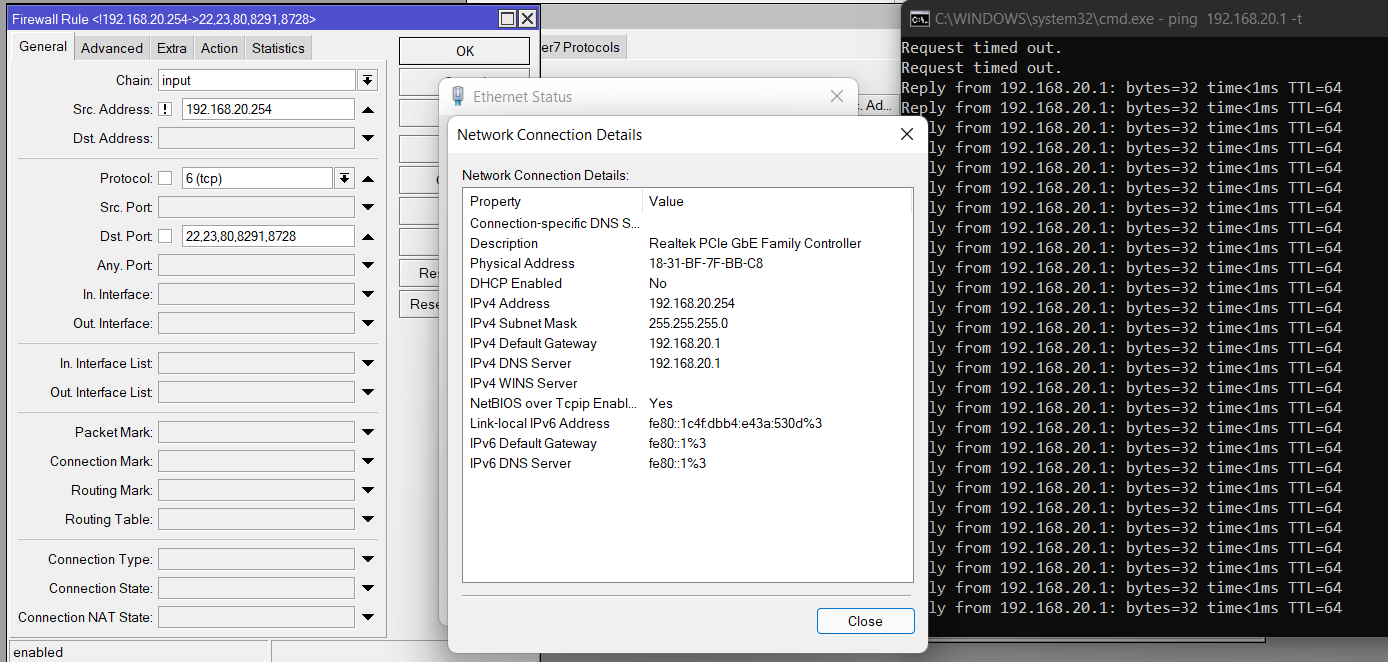
Gambar 4.16 Pengujian Saat ISP Utama Mengalami Gangguan

Tabel 4.2 Hasil Pengujian Automatic Failover

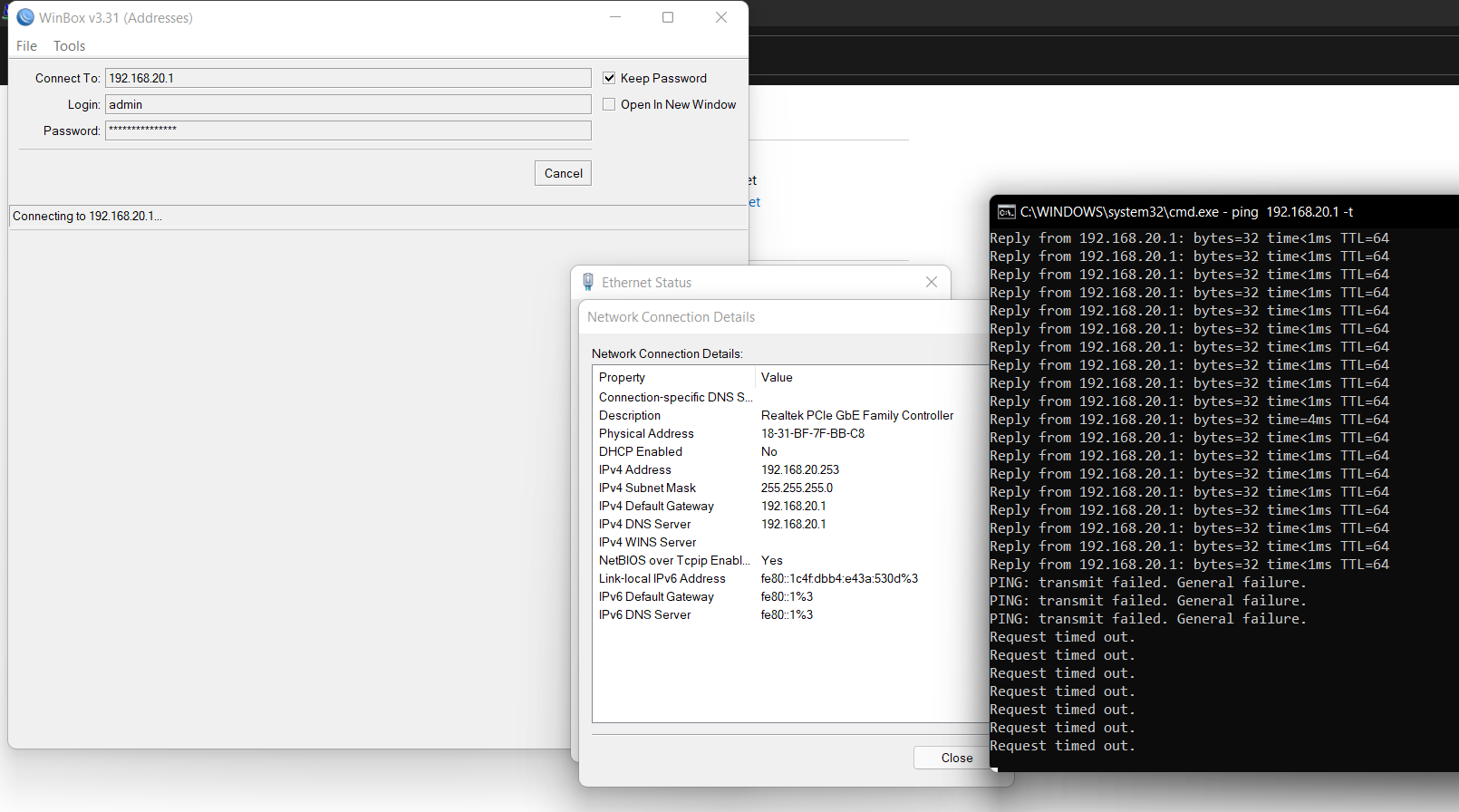
|  |  |  |
| --- | --- | --- |
| Status | | Keterangan |
| ISP Utama (Biznet) | ISP Backup (Telkom) |
| Hidup | Hidup | Koneksi berjalan dengan baik |
| Mati | Hidup | Koneksi berjalan dengan baik |
| Hidup | Mati | Koneksi berjalan dengan baik |

### Pengujian Keamanan Jaringan

Tahapan pengujian kemanan jaringan ini diUji dengan melakukan konfigurasi IP pada komputer admin dengan menggunakan IP address admin 192.168.20.254 dapat melakukan ping ke router mikrotik dan dapat mengakses mikrotik .



Gambar 4.17 Pengujian Akses Router dan Pengecekan Ping

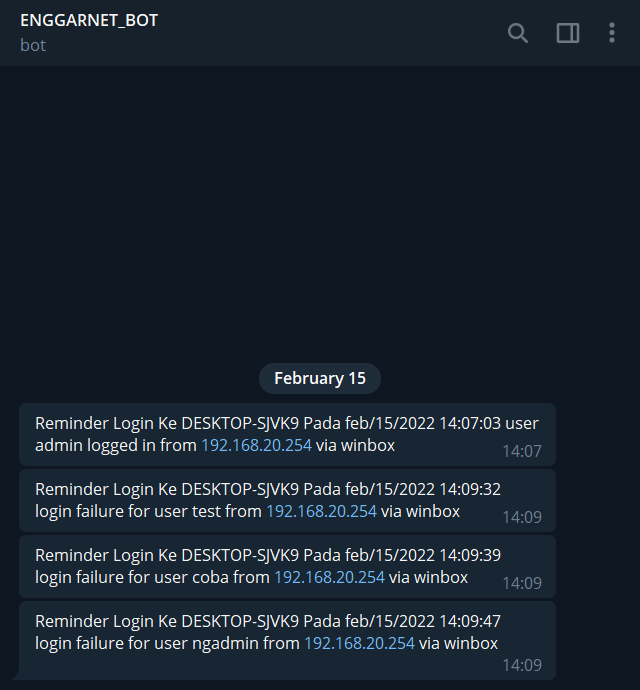


Gambar 4.18 Pengujian Akses Router dan Pengecekan Ping

Tahapan kedua pengujian kemanan jaringan ini diUji dengan melakukan konfigurasi IP pada komputer admin dengan menggunakan *IP address* selain ip admin, yaitu 192.168.20.253 tidak dapat melakukan ping ke router mikrotik dan tidak dapat mengakses mikrotik .

### Pengujian Notifikasi Admin

Tahapan pengujian Notifikasi unuk Admin ini diUji dengan melakukan percobaan *login* asal terhadap router, sehingga aktifikas percobaan masuk kedalam router akan terbaca oleh scheduler lalu *scheduler* akan memberikan notifikasi ke Admin melalui Bot Telegram.



Gambar 4.19 Hasil Notifikasi Admin

Gambar diatas menunjukkan Notifikasi ke Admin dari aktifitas yang mencurigakan terhadap jaringan yang dilakukan dengan percobaan *login*. Dari hasil notifikasi, terdapat info nama *device* yang dicoba, tanggal, *user* yang digunakan, IP yang digunakan pengguna, dan aplikasi yang digunakan.

# **BAB V**

# **PENUTUP**

## Kesimpulan

Berdasarkan pada pembahasan serta uraian yang telah dijelaskan dalam bab-bab sebelumnya perihal dari latar belakang masalah pada penelitian terdahulu , implementasi automatic failover tidak dengan recursive gateway yang mengakibatkan pengecekan hanya antara mikrotik dengan modem isp, tidak adanya keamanan jaringan sehingga dapat mengakibatkan komputer selain admin dapat mengakses router mikrotik dan device lain yang terhubung dan uji coba yang telah dibentuk, maka penulis menyimpulkan berdasarkan hasil pengujian yang dilakukan, implementasi automatic failover dengan recursive gateway untuk otomatis memindahkan jalur utama ke jalur backup menggunakan pengecekan ping ke gateway isp. Keamanan jaringan menggunakan firewall filtering dengan memblokir IP selain admin untuk mengakses router dan device lain bisa mencegah user lain untuk melakukan penyerangan, pencurian data, dan merusak jaringan dan adanya monitoring Log memberikan notifikasi untuk admin jika terdapat user yang mencurigakan sedang mengakses jaringan.

## Saran

Saran-saran yang diajukan agar menjadi masukan untuk pengembangan  
berikutnya adalah sebagai berikut:

1. Untuk pengembangan selanjutnya perlu penambahan *port blocking* untuk memperkuat kemanan jaringan.

**DAFTAR PUSTAKA**

Adhi Purwaningrum, F., Purwanto, A., Agus Darmadi, E., Tri Mitra Karya Mandiri Blok Semper Jomin Baru, P., & -Karawang, C. (2018). *Optimalisasi Jaringan Menggunakan Firewall*. *2*(3), 17–23.

Purnama. (2019). Optimalisasi Keamanan Jaringan Wireless Menggunakan Firewall Filtering MAC Address. *Indonesian Journal On Networking and Security*, *8*(4), 43–47.

Mora, M. (2014). OPTIMALISASI MANAJEMEN JARINGAN DENGAN MENGGUNAKAN Mikrotik RouterOS. *Jurnal Sistem Informasi Universitas Suryadarma*, *2*(1). https://doi.org/10.35968/jsi.v2i1.82

Dan, F., Bandwith, M., Pt, P., Prima, I., Supendar, H., & Sw, S. (2020). *Optimalisasi Sistem Keamanan Jaringan Komputer Menggunakan Metode*. *21*(1), 104–111.

Langobelen, E. S. R. O. B., Rachmawati, Y., & Iswahyudi, C. (2019). Analisis Dan Optimasi Dari Simulasi Keamanan Jaringan Menggunakan Firewall Mikrotik Studi Kasus Di Taman Pintar Yogyakarta. *Jurnal JARKOM*, *7*(2), 95–102.

Muzakir, A., & Ulfa, M. (2019). Analisis Kinerja Packet Filtering Berbasis Mikrotik Routerboard Pada Sistem Keamanan Jaringan. *Simetris: Jurnal Teknik Mesin, Elektro Dan Ilmu Komputer*, *10*(1), 15–20. https://doi.org/10.24176/simet.v10i1.2646

Mohammad Badrul, A. (2019). Implementasi Automatic Failover Menggunakan Router Jaringan Mikrotik Untuk Optimalisasi Jaringan. *Jurnal PROSISKO*, *6*(2), 82–87.

Novianto, D., & Helmud, E. (2019). Implementasi Failover dengan Metode Recursive Gateway Berbasis Router Mikrotik Pada STMIK Atma Luhur Pangkalpinang. *Jurnal Ilmiah Informatika Global*, *10*(1), 26–31. https://doi.org/10.36982/jig.v10i1.732

Rizal, R., Ruuhwan, R., & Nugraha, K. A. (2020). Implementasi Keamanan Jaringan Menggunakan Metode Port Blocking dan Port Knocking Pada Mikrotik RB-941. *Jurnal ICT : Information Communication & Technology*, *19*(1), 1–8. https://doi.org/10.36054/jict-ikmi.v19i1.119

Irawati, & Indrarini, D. (2015). *Jaringan Komputer dan Data Lanjut.* Yogyakarta: Deepublish.

Kustanto, & Saputro, D. T. (2015). *Belajar Jaringan Komputer Berbasis Mikrotik OS Edisi Revisi.* Yogyakarta: Gava Media.

Madcom. (2010). *Sistem Jaringan Komputer untuk Pemula.* Yogyakarta: Andi Publisher.

**LAMPIRAN KONFIGURASI**

|  |
| --- |
| /ip firewall mangle  add action=mark-connection chain=input in-interface="1.ISP-UTAMA" new-connection-mark="M-ISPUTAMA" passthrough=yes  add action=mark-connection chain=input in-interface="2.ISP-BACKUP" new-connection-mark="M-ISPBACKUP" passthrough=yes  add action=mark-routing chain=output connection-mark="M-ISPUTAMA" new-routing-mark="TO-ISPUTAMA" passthrough=yes  add action=mark-routing chain=output connection-mark="M-ISPBACKUP" new-routing-mark="TO-ISPBACKUP" passthrough=yes  add action=mark-connection chain=prerouting dst-address-list=!LOCAL-IP dst-address-type=!local new-connection-mark="M-ISPUTAMA" passthrough=yes per-connection-classifier=both-addresses-and-ports:2/0 src-address-list=LOCAL-IP  add action=mark-connection chain=prerouting dst-address-list=!LOCAL-IP dst-address-type=!local new-connection-mark="M-ISPBACKUP " passthrough=yes per-connection-classifier=both-addresses-and-ports:2/1 src-address-list=LOCAL-IP  add action=mark-routing chain=prerouting connection-mark="M-ISPUTAMA" dst-address-list=!LOCAL-IP new-routing-mark="TO-ISPUTAMA" passthrough=yes src-address-list=LOCAL-IP add action=mark-routing chain=prerouting connection-mark="M-ISPBACKUP" dst-address-list=!LOCAL-IP new-routing-mark="TO-ISPBACKUP" passthrough=yes src-address-list=LOCAL-IP |

|  |
| --- |
| /ip route add dst-address="0.0.0.0/0" target-scope="30" distance="1" gateway="8.8.8.8" comment="1.ISP-UTAMA" check-gateway="ping" scope="30" add dst-address="0.0.0.0/0" target-scope="30" distance="2" gateway="1.1.1.1" comment="2.ISP-BACKUP" check-gateway="ping" scope="30" add dst-address="8.8.8.8" target-scope="10" distance="1" gateway="192.168.19.1" comment="1.ISP-UTAMA-Check" check-gateway="ping" scope="30" add dst-address="1.1.1.1" target-scope="10" distance="1" gateway="192.168.8.1" comment="2.ISP-BACKUP-Check" check-gateway="ping" scope="30" |

|  |
| --- |
| /ip firewall filter  add chain=input action=drop protocol=tcp src-address=**!192.168.20.21** dst-port=22,23,80,8291,8728  add chain=input action=drop protocol=tcp src-address=**192.168.20.2-192.168.20.254** dst-address=**192.168.20.1** |

|  |
| --- |
| # BEGIN SETUP  :local myserver ([/system identity get name])  :local scheduleName "NotifikasiAdmin"  local bot "5107234528:AAEhPSZ65g9TmGsrwKT5yP9HYPP\_Cqr6GsM"  local ChatID "924095064"  :local startBuf [:toarray [/log find message~"logged in" || message~"login failure"]]  # END SETUP  # get last time  :local lastTime [/system scheduler get [find name="$scheduleName"] comment]  # for checking time of each log entry  :local currentTime  # log message  :local message    # final output  :local output  :local keepOutput false  # if lastTime is empty, set keepOutput to true  :if ([:len $lastTime] = 0) do={  :set keepOutput true  }  :local counter 0  # loop through all log entries that have been found  :foreach i in=$startBuf do={    # loop through all removeThese array items  :local keepLog true  :foreach j in=$removeThese do={  # if this log entry contains any of them, it will be ignored  :if ([/log get $i message] ~ "$j") do={  :set keepLog false  }  }  :if ($keepLog = true) do={    :set message [/log get $i message]  # LOG DATE  # depending on log date/time, the format may be different. 3 known formats  # format of jan/01/2002 00:00:00 which shows up at unknown date/time. Using as default  :set currentTime [ /log get $i time ]  # format of 00:00:00 which shows up on current day's logs  :if ([:len $currentTime] = 8 ) do={  :set currentTime ([:pick [/system clock get date] 0 11]." ".$currentTime)  } else={  # format of jan/01 00:00:00 which shows up on previous day's logs  :if ([:len $currentTime] = 15 ) do={  :set currentTime ([:pick $currentTime 0 6]."/".[:pick [/system clock get date] 7 11]." ".[:pick $currentTime 7 15])  }  }    # if keepOutput is true, add this log entry to output  :if ($keepOutput = true) do={  :set output ($output.$currentTime." ".$message."\r\n")  }  :if ($currentTime = $lastTime) do={  :set keepOutput true  :set output ""  }  }  :if ($counter = ([:len $startBuf]-1)) do={  :if ($keepOutput = false) do={  :if ([:len $message] > 0) do={  :set output ($output.$currentTime." ".$message."\r\n")  }  }  }  :set counter ($counter + 1)  }  if ([:len $output] > 0) do={  /system scheduler set [find name="$scheduleName"] comment=$currentTime  /tool fetch url="https://api.telegram.org/bot5107234528:AAEhPSZ65g9TmGsrwKT5yP9HYPP\_Cqr6GsM/sendmessage?chat\_id=924095064&text=Reminder Login Ke $myserver Pada $currentTime $message" keep-result=no;  } |