OPTIMALISASI JARINGAN INTERNET MENGGUNAKAN MIKROTIK DI BALAI RISET DAN STANDARDISASI INDUSTRI SURABAYA

KERJA PRAKTIK

Program Studi
S1 Teknik Komputer

Oleh :
Yosia Pradeska Admaja
17410200022

FAKULTAS TEKNOLOGI DAN INFORMATIKA
UNIVERSITAS DINAMIKA
2021

OPTIMALISASI JARINGAN INTERNET MENGGUNAKAN MIKROTIK DI BALAI RISET DAN STANDARDISASI INDUSTRI SURABAYA

Diajukan sebagai salah satu syarat untuk menyelesaikan
mata kuliah Kerja Praktik

Disusun oleh :

Nama : Yosia Pradeska Admaja

NIM : 17410200022

Program : S1 (Strata Satu)

Jurusan : Teknik Komputer

FAKULTAS TEKNOLOGI DAN INFORMATIKA

UNIVERSITAS DINAMIKA

2021

HALAMAN PENGESAHAN

LEMBAR PENGESAHAN

OPTIMALISASI JARINGAN INTERNET MENGGUNAKAN MIKROTIK DI BALAI RISET DAN STANDARDISASI INDUSTRI SURABAYA

Laporan Kerja Praktik oleh

Yosia Pradeska Admaja

NIM : 17410200022

Telah diperiksa, diuji dan disetujui

Surabaya, Januari 2021

Disetujui :

Dosen Pembimbing,

Weny Indah Kusumawati, S.Kom., M.MT.

NIDN. 0721047201

Penyelia,

Fatimah, S.E., M.M.

NIP. 196403151991032001

Mengetahui,

Ketua Program Studi S1 Teknik Komputer

Digitally signed by Universitas Dinamika
Date: 2021.01.07 08:33:08 +07'00'

Pauladie Susanto, S.Kom., M.T.

NIDN. 0729047501

SURAT PERNYATAAN

PERSETUJUAN PUBLIKASI DAN KEASLIAN KARYA ILMIAH

Sebagai mahasiswa Universitas Dinamika, saya :

Nama	:	Yosia Pradeska Admaja
NIM	:	17410200022
Program Studi	:	S1 Teknik Komputer
Fakultas	:	Fakultas Teknologi dan Informatika
Jenis Karya	:	Laporan Kerja Praktik
Judul Karya	:	**OPTIMALISASI JARINGAN INTERNET MENGGUNAKAN MIKROTIK DI BALAI RISET DAN STANDARDISASI INDUSTRI SURABAYA**

Menyatakan dengan sesungguhnya bahwa:

1. Demi pengembangan Ilmu Pengetahuan, Teknologi dan Seni, saya menyetujui memberikan kepada Universitas Dinamika Hak Bebas Royalti Non-Eksklusif (*Non-Exclusive Royalti Free Right)* atas seluruh isi/ sebagian karya ilmiah saya tersebut di atas untuk disimpan, dialihmediakan dan dikelola dalam bentuk pangkalan data *(database)* untuk selanjutnya didistribusikan atau dipublikasikan demi kepentingan akademis dengan tetap mencantumkan nama saya sebagai penulis atau pencipta dan sebagai pemilik Hak Cipta
2. Karya tersebut di atas adalah karya asli saya, bukan plagiat baik sebagian maupun keseluruhan. Kutipan, karya atau pendapat orang lain yang ada dalam karya ilmiah ini adalah semata hanya rujukan yang dicantumkan dalam Daftar Pustaka saya
3. Apabila dikemudian hari ditemukan dan terbukti terdapat tindakan plagiat pada karya ilmiah ini, maka saya bersedia untuk menerima pencabutan terhadap gelar kesarjanaan yang telah diberikan kepada saya.

Demikian surat pernyataan ini saya buat dengan sebenarnya.

Surabaya, 7 Januari 2021

Yang menyatakan,

Yosia Pradeska Admaja

NIM : 17.41020.0022

ABSTRAK

Optimalisasi jaringan internet menggunakan MikroTik di Balai Riset dan Standardisasi Industri Surabaya merupakan suatu langkah yang digunakan untuk membantu memberikan serta menyajikan informasi yang diperlukan oleh admin jaringan mengenai kondisi penggunaan jaringan internet di kantor instansi tersebut. Optimalisasi ini memanfaatkan fitur *router* yang sudah disediakan, fitur tersebut meliputi aspek keamanan, performa, dan pemantauan. Optimalisasi ini sangat membantu admin jaringan untuk memaksimalkan dan memantau penggunaan jaringan internetnya serta proses *teleconference* yang dilakukan oleh pegawai akan menjadi lebih efektif dan efisien.

Proses optimalisasi ini menggunakan fitur *firewall* dan *mangle* sebagai kunci utama untuk memisahkan antara *traffic browsing* dengan *traffic teleconference.* Selain itu, pemanfaatan fitur keamanan juga akan diterapkan sehingga *router* tidak bisa diretas oleh pihak tidak bertanggung jawab. Untuk meringankan beban kerja admin jaringan maka ditambahkan juga fitur pemantauan *access point*. Jenis r*outer* yang digunakan adalah MikroTik RB11004AhX dengan integrasi WinBox untuk mengakses *router.*

Kata Kunci : Optimalisasi jaringan, MikroTik, *teleconference, firewall, mangle,* BARISTAND Industri Surabaya.

KATA PENGANTAR

Puji syukur atas kehadirat Tuhan Yang Maha Esa karena atas rahmat dan karunia-Nya, penulis dapat menyelesaikan laporan Kerja Praktik yang berjudul "Optimalisasi Jaringan Internet Menggunakan MikroTik Di Balai Riset dan Standardisasi Industri Surabaya". Laporan ini disusun berdasarkan hasil studi dalam pelaksanaan Kerja Praktik di Balai Riset dan Standardisasi Industri Surabaya yang dilakukan selama satu bulan.

Dalam pelaksanaan Kerja Praktik dan penyelesaian laporan Kerja Praktik ini, penulis memperoleh bantuan dari berbagai pihak yang telah memberikan dukungan, baik berupa dukungan materil maupun dukungan moril. Oleh karena itu, pada kesempatan ini penulis mengucapkan terima kasih kepada:

1. Orang tua dan keluarga besar penulis yang selalu memberikan dukungan dan motivasi kepada penulis.
2. Bapak Pauladie Susanto, S.Kom., M.T., selaku Ketua Program Studi S1 Teknik Komputer yang telah memberikan arahan selama pelaksanaan Kerja Praktik.
3. Ibu Weny Indah Kusumawati, S.Kom., M.MT., selaku Dosen Pembimbing yang telah memberikan dukungan berupa motivasi, saran, dan wawasan bagi penulis selama pelaksanaan Kerja Praktik dan pembuatan laporan Kerja Praktik.
4. Ibu Fatimah S.E., M.M., selaku Kepala Seksi Pengembangan Jasa Teknik dan penyelia penulis yang telah memberikan ijin selama pelaksanaan Kerja Praktik.

5. Ibu Nurzaitun Purwasih dan Mas Azhar selaku pembimbing penulis selama melakukan Kerja Praktik.

Semoga Tuhan Yang Maha Esa memberikan rahmat-Nya kepada seluruh pihak yang membantu penulis dalam pelaksanaan Kerja Praktik dan penyelesaian laporan Kerja Praktik. Penulis menyadari di dalam laporan Kerja Praktik ini masih banyak kekurangan, meskipun demikian penulis tetap berharap laporan Kerja Praktik ini bermanfaat bagi penulis dan semua pihak. Oleh karena itu, adanya saran dan kritik sangat diharapkan.

Surabaya, 23 November 2020

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Balai Riset dan Standardisasi Industri Surabaya memiliki jaringan internet yang memudahkan pegawainya untuk menunjang kegiatan selama bekerja. Tidak hanya itu, jaringan internet nirkabel berupa wi-fi (*wireless fidelity*) ini juga dapat diakses gratis oleh pelanggan dan tamu sebagai bentuk pelayanan dari instansi. Jaringan komputer (c*omputer network*) adalah jaringan dari sistem komunikasi data yang melibatkan sebuah atau lebih sistem komputer yang dihubungkan dengan jalur transmisi alat komunikasi yang membentuk suatu sistem. Dengan jaringan, sebuah komputer dapat menggunakan data di komputer lain, dapat mencetak laporan di printer komputer lain, dan dapat memberi berita ke komputer lain walaupun pada area yang berbeda.

Bagi sebuah instansi yang mempunyai tugas melaksanakan riset dan Standardisasi serta sertifikasi di bidang industri elektronika telematika, maka instansi tersebut memerlukan teknologi internet untuk kegiatan penelitian dan pengembangan teknologi industri elektronika telematika, baik antar departemen atau kantor pusat yang berada di wilayah lain. Oleh karena itu instansi ini sangat perlu didukung dengan performa teknologi jaringan internet yang baik. Jika manajemen jaringannya belum berjalan dengan baik, hal ini menyebabkan timbulnya beberapa masalah dalam menjalankan operasinya setiap hari, seperti belum adanya pembagian *IP address* yang ideal, sehingga akan menimbulkan *IP conflict* dan kehabisan *IP address* yang akan mengganggu kelancaran jaringan

baik untuk jaringan lokal maupun internet. Belum adanya pembagian *bandwidth* internet yang ideal untuk keperluan *teleconference*, sehingga *traffic* jaringan internet menjadi tidak stabil ketika digunakan untuk keperluan *teleconference*. Serta belum diterapkannya keamanan dalam jaringan, sehingga sangat rentan akan gangguan baik berupa pencurian data, maupun gangguan lainnya yang dapat membahayakan *router*.

Untuk mengatasi masalah tersebut, perlu dilakukan pengimplementasian manajemen jaringan berbasis MikroTik RouterOS. Diharapkan dengan mengimplementasikan sistem jaringan yang baru nanti dapat berfungsi lebih efektif dan dapat mengatasi masalah – masalah yang terdapat pada sistem jaringan yang ada.

1.2 Rumusan Masalah

Berdasarkan uraian dari latar belakang tersebut, maka dapat dirumuskan permasalahan yang ada, yaitu bagaimana memaksimalkan kinerja perangkat *router* dari segi performa untuk kebutuhan *teleconference*, keamanan, dan fitur yang dimiliki.

1.3 Batasan Masalah

Batasan masalah pada Optimalisasi Jaringan Internet Menggunakan MikroTik di Balai Riset dan Standardisasi Industri Surabaya adalah sebagai berikut:

1. Melakukan konfigurasi sistem keamanan jaringan menggunakan MikroTik.

2. Membuat *mangle rule* untuk memisahkan keperluan *traffic browsing* dengan *traffic teleconference.*
3. Menerapkan monitoring *Access Point* menggunakan fitur *Netwatch.*

1.4 Tujuan

Berdasarkan perumusan masalah di atas, maka akan diterapkan konfigurasi untuk memaksimalkan kinerja *router* dari sisi performa, keamanan, dan fitur. Sehingga memberikan kemudahan pegawai perusahaan dalam melakukan kegiatan *teleconference*, dan juga mempermudah admin jaringan untuk memantau kondisi perangkat *Access Point* yang ada.

1.5 Manfaat

1. Bagi Mahasiswa
   a. Dapat memahami berbagai alur kerja yang ada di instansi pemerintah.
   b. Menambah wawasan dan pengetahuan untuk membekali diri baik *hard skill* ataupun *soft skill* yang diperlukan di dunia kerja.
   c. Dapat menerapkan serta mengembangkan ilmu yang telah dipelajari selama perkuliahan.
   d. Menambah relasi dengan pegawai di instansi.
2. Bagi Instansi
   a. Menjalin hubungan erat antara instansi dengan perguruan tinggi.
   b. Instansi mendapat bantuan tenaga kerja dari mahasiswa, sehingga beberapa permasalahan di instansi bisa terselesaikan.
   c. Meringankan beban kerja admin jaringan.

BAB II

GAMBARAN UMUM INSTANSI

2.1 Gambaran Umum Balai Riset dan Stadardisasi Industri Surabaya

Balai Riset dan Standardisasi Industri Surabaya yang kemudian disebut sebagai BARISTAND Surabaya adalah sebuah instansi pemerintahan yang mempunyai tugas melaksanakan riset dan Standardisasi serta sertifikasi di bidang industri elektronika telematika. BARISTAND Industri Surabaya berlokasi di Jalan Jagir Wonokromo 360, Surabaya. BARISTAND Industri Surabaya sebagai unit pelaksana teknis yang menangani penelitian dan pengembangan industri elektronika telematika, berperan dalam melaksanakan kebijakan pengembangan industri nasional untuk menopang pengembangan industri elektronika telematika di Indonesia. Dengan melaksanakan tugas tersebut maka diharapkan akan berkembang industri elektronika telematika yang kuat dan mandiri sehingga dapat memperluas lapangan kerja dan mendorong percepatan pembangunan industri nasional.

2.2 Logo BARISTAND Industri Surabaya

Berikut ini adalah logo resmi yang dimiliki oleh BARISTAND Industri Surabaya pada gambar 1:

Gambar 1 Logo BARISTAND Industri Surabaya

2.3 Visi BARISTAND Industri Surabaya

Visi BARISTAND Industri Surabaya merupakan potret masa depan yang dicita-citakan yaitu Sebagai Lembaga Riset dan Standardisasi Industri terkemuka, yang menjadi mitra industri elektronika dan telematika nasional dalam berperan sebagai basis produksi yang melayani kebutuhan nasional maupun dunia pada tahun 2025.

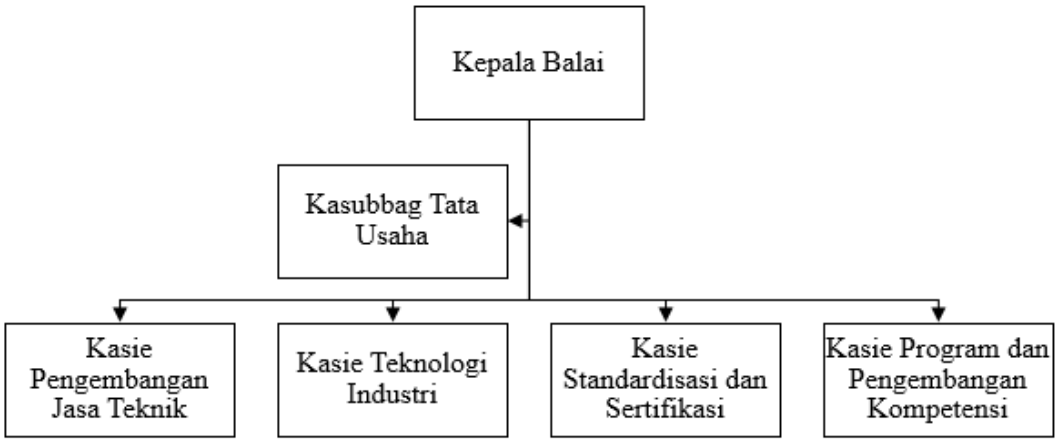
2.4 Misi BARISTAND Industri Surabaya

BARISTAND Industri Surabaya dalam usaha keras mencapai Visi yang telah ditetapkan diatas, mengemban Misi sebagai berikut:

1. Menghasilkan riset dan rancang bangun perekayasaan industri elektronika dan telematika.
2. Menghasilkan pelayanan kesesuaian (pengujian, kalibrasi dan sertifikasi) produk industri elektronika dan telematika.
3. Mengembangkan kompetensi sumber daya manusia pada industri elektronika dan telematika.

2.5 Struktur Organisasi BARISTAND Industri Surabaya

BARISTAND Industri Surabaya terdapat beberapa bagian yang memiliki tanggung jawab masing-masing kegiatan bisnis yang ada. Semua bagian bertanggung jawab langsung kepada Kepala Balai, dapat dilihat pada Gambar 2.



Gambar 2 Struktur organisasi BARISTAND Industri Surabaya

2.6 Deskripsi Tugas Bagian

Berdasarkan struktur organisasi pada gambar 2 dapat dideskripsikan tugas yang dimiliki oleh tiap bagian yang bersangkutan sebagai berikut:

1. Kepala Balai

   Mempunyai tugas pokok memimpin, mengkoordinasikan dan mengendalikan pelaksanaan kegiatan di BARISTAND Industri Surabaya.

2. Kasubbag Tata Usaha

   Melakukan pengawasan terkait dengan urusan kepegawaian, keuangan, inventarisasi barang milik negara, tata persuratan, perlengkapan, kearsipan, rumah tangga, koordinasi penyusunan bahan rencana dan program, penyiapan bahan evaluasi dan pelaporan BARISTAND Industri, serta pengelolaan perpustakaan.

3. Kasie Pengembangan Jasa Teknis

   Melakukan pengawasan terkait dengan penyiapan bahan pemasaran, kerjasama, promosi, pelayanan informasi, penyebarluasan, dan pendayagunaan hasil penelitian dan pengembangan.

4. Kasie Teknologi Industri

   Melakukan pengawasan terkait dengan penyiapan bahan penelitian dan pengembangan teknologi industri bahan baku, bahan penolong, proses, peralatan atau mesin, dan hasil produk, serta penanggulangan pencemaran industri.

5. Kasie Standardisasi dan Sertifikasi

   Melakukan pengawasan terkait dengan penyiapan bahan perumusan dan penerapan standar, pengujian dan sertifikasi dalam bidang bahan baku, bahan penolong, proses, peralatan atau mesin, dan hasil produk.

6. Kasie Program dan Pengembangan Kompetensi

   Melakukan pengawasan terkait dengan penyiapan bahan penyusunan program dan pengembangan kompetensi di bidang jasa riset atau penelitian dan pengembangan.

BAB III

LANDASAN TEORI

3.1 Jaringan Komputer

Jaringan Komputer adalah sekelompok komputer otonom yang saling menggunakan protokol komunasi melalui media komunikasi, sehingga dapat berbagi data, informasi, program aplikasi, dan perangkat keras seperti *printer*, *scanner* ataupun *hardisk*, serta memungkinkan untuk saling berkomunikasi secara elektronik. Jaringan komputer dapat dikelompokkan berdasarkan media transmisi yang dapat digunakan. Secara umum jaringan komputer terbagi menjadi 2 jenis, yaitu Jaringan Berkabel (*Wired Network)* dan Jaringan Nirkabel *(Wireless Network).*

1. Jaringan Berkabel (*Wired Network)*

   Wired Network merupakan media transmisi menggunakan kabel untuk menghubungkan antar komputer. Media transmisi ini bekerja dengan cara mengirimkan informasi dalam bentuk sinyal listrik. Dan memiliki kemampuan transfer data yang cepat, dan biasanya digunakan dalam area lokal, misalnya dalam satu gedung atau antar gedung. Kabel yang sering digunakan sebagai media transmisi antara lain: *twisted pair, coaxial, fiber optic,* dan sebagainya.

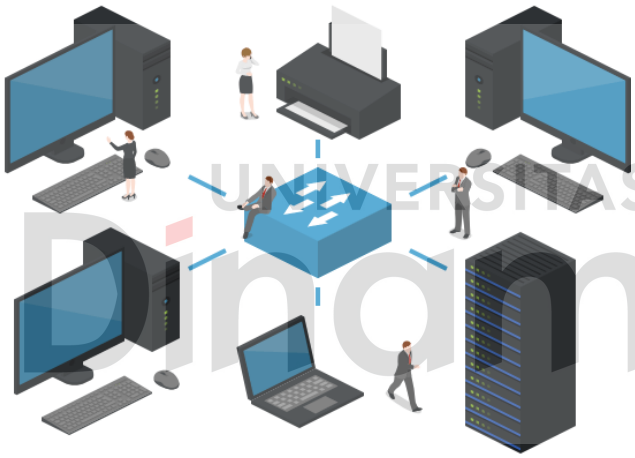
2. Jaringan Nirkabel *(Wireless Network)*

   Wireless Network adalah media transmisi yang memanfaatkan gelombang elektromagnetik sebagai komunikasi datanya. Media transmisi tanpa kabel ini dapat diakses oleh pengguna dimanapun berada, namun kemampuan transfer datanya lebih kecil dibandingkan dengan jaringan kabel.

Jika sumber data dan penerima data memiliki jarak yang jauh atau medannya sulit, maka bisa digunakan media transmisi radiasi elektromagnetik yang dipancarkan lewat udara terbuka berupa *gelombang mikro dan gelombang radio.*

Selain itu, jaringan komputer juga dikelompokkan berdasarkan luas area yang dapat dijangkau atau dilayani. Secara umum jaringan komputer terbagi menjadi 3 jenis, yaitu *Local Area Network (LAN), Metropolitan Area Network (MAN), dan Wide Area Network (WAN).*

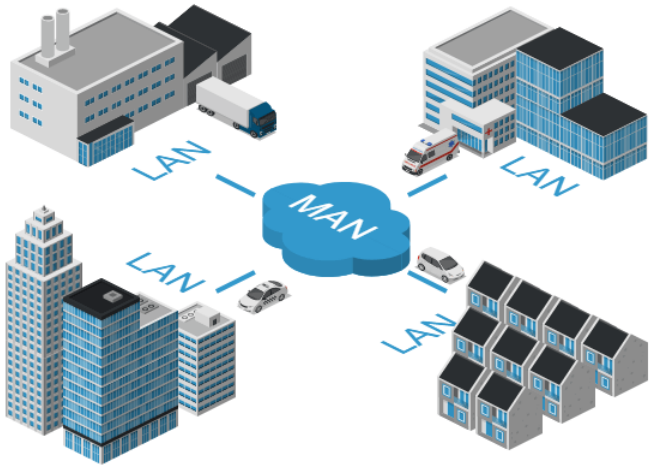
1. *Local Area Network (LAN)*



Gambar 3 Jaringan *LAN*

Local Area Network merupakan jaringan komputer dengan luasan area lokal yang *terbatas* seperti pada area perkantoran, perumahan atau sekolah atau bisa disebut juga selama jaringan komputer tersebut berada pada 1 area yang sama dari sebuah institusi atau instansi. Pada umumnya *Local Area Network* menggunakan media transmisi berupa kabel UTP atau *wireless* radio. Serta menggunakan topologi tertentu dimana beberapa komputer terhubung ke perangkat switch, dan memiliki cakupan luas maksimal 1 kilometer.

2. *Metropolitan Area Network (MAN)*



Gambar 4 Jaringan *MAN*

Metropolitan Area Network menghubungkan jaringan komputer pada luas area seukuran kota. Metropolitan *Area Network* akan menghubungkan antar *Local Area Network* yang ada pada beberapa lokasi yang berjauhan namun masih dalam lingkup 1 kota sehingga pengguna dapat berbagi sumber daya dengan pengguna lain di lokasi yang lain. Biasanya digunakan pada perusahaan yang memiliki cabang di beberapa lokasi namun masih dalam wilayah 1 kota.

3. *Wide Area Network (WAN).*

Gambar 5 Jaringan *WAN*

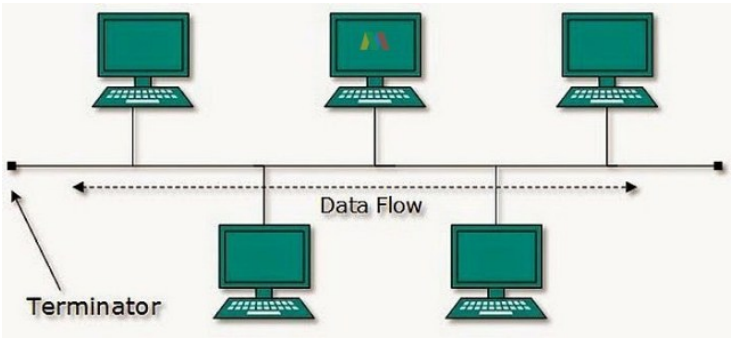
Wide Area Network merupakan jaringan komputer terbesar yang menghubungkan banyak *Metropolitan Area Network*. Pada *Wide Area Network* menggunakan berbagai teknologi media transmisi mulai dari *submarine fiber optic* (*fiber optic* bawah laut) sampai ke komunikasi satelit. Teknologi yang digunakan untuk menghubungkan beberapa kantor cabang perusahaan adalah *Virtual Private Network* atau sering disebut juga dengan *tunneling*. Dengan menggunakan teknologi *VPN/Tunneling* pengguna tidak perlu mengetahui media transmisi yang digunakan sehingga dapat terhubung ke kantor pusat yang berada di negara lain.

3.2 Topologi Jaringan Komputer

Topologi jaringan komputer adalah hal yang menjelaskan hubungan geometris antara unsur-unsur dasar penyusun jaringan, yaitu *node, link,* dan *station.* Pada umumnya, topologi jaringan dibagi menjadi 5 pola, yaitu Topologi

Bus, Topologi *Ring,* Topologi *Star,* Topologi *Tree,* dan Topologi *Mesh*. Berikut penjelasannya:

2. Topologi *Bus*

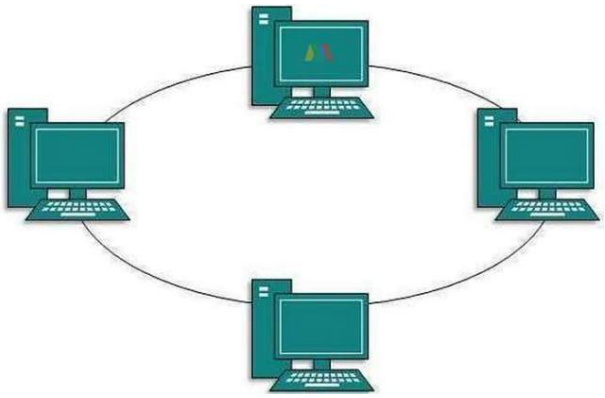


Gambar 6 Topologi *Bus*

Topologi *Bus* adalah topologi jaringan yang sederhana. Pada umumnya topologi jaringan ini dilakukan pada installasi jaringan berbasis kabel *coaxial* pada sepanjang node *client* dan konektor. Jenis konektor yang digunakan salah satunya adalah *Terminator*. Jenis topologi ini biasanya digunakan untuk jaringan komputer perusahaan dengan skala kecil. Karakteristik khusus topologi *bus* yaitu penggunaan kabel tunggal yang terbentang di sepanjang jaringan dan berfungsi sebagai kabel utama (*backbone*).

Setiap perangkat komputer terhubung dengan kabel utama *(backbone)* dimana masing-masing komputer dapat saling berkirim dan menerima paket data. Proses pengiriman paket data antar komputer hanya dapat dilakukan ketika kabel utama dalam keadaan bebas dimana komputer lain sedang tidak melakukan pertukaran data. Pengiriman data dari suatu komputer ke komputer lainnya dilakukan dengan menggunakan sinyal yang tersebar di kabel jaringan. Hanya komputer dengan *IP* atau alamat *MAC* yang sama dengan yang dituju yang akan menerima sinyal.

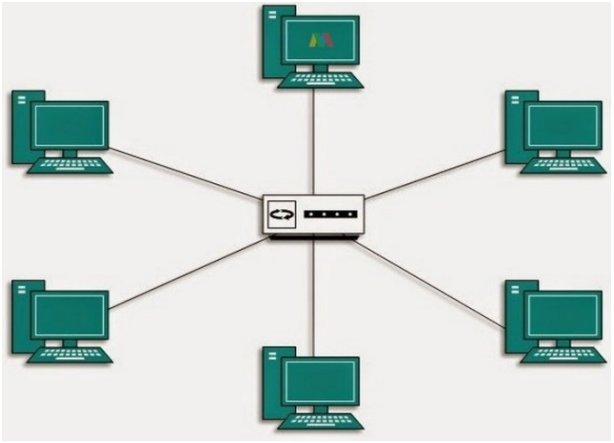
3. Topologi *Ring*



Gambar 7 Topologi *Ring*

Topologi *ring* atau sering disebut dengan topologi cincin merupakan topologi jaringan yang dipakai untuk menghubungkan sebuah komputer dengan komputer lainnya dalam sebuah rangkaian yang berbentuk melingkar seperti cincin. Jenis topologi jaringan ini umumnya hanya menggunakan *LAN card* agar masing-masing komputer terkoneksi. Jenis topologi ini paling banyak digunakan di lingkungan perkantoran atau perusahaan. Secara umum, topologi ring memiliki karakteristik khusus, yaitu menggunakan kabel tipe UTP dan *Patch Cable* yang membentuk jaringan seperti lingkaran dan terdiri dari beberapa *node* yang disusun secara seri.

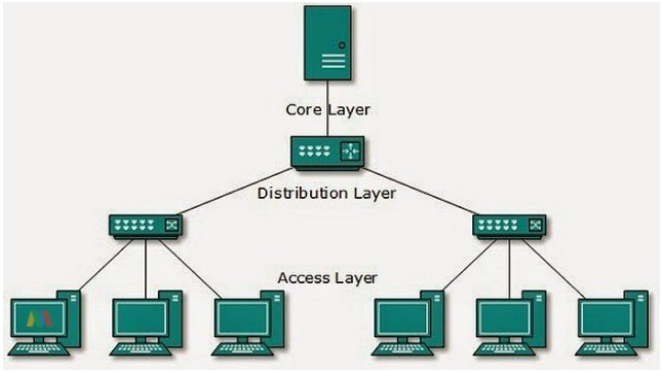
4. Topologi *Star*



Gambar 8 Topologi *Star*

Topologi *star* atau disebut juga dengan topologi bintang adalah topologi jaringan berbentuk bintang dimana pada umumnya memakai *hub* atau *switch* untuk koneksi antar client. Topologi jaringan komputer ini paling sering digunakan saat ini karena memiliki banyak kelebihan. Jenis topologi ini juga cukup banyak digunakan di perkantoran atau perusahaan dengan skala kecil dan menengah. Karaktersitik khusus dari topologi *star* adalah adanya satu jaringan yang berfungsi sebagai pusat segala aktivitas, dimana setiap komputer memiliki kabel tersendiri yang terkoneksi langsung dengan perangkat *hub* atau *switch* dengan sistem *point-to-point.*

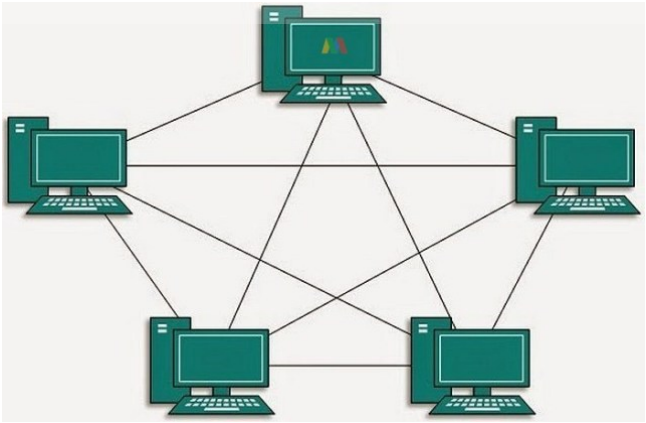
5. Topologi *Tree*



Gambar 9 Topologi *Tree*

Topologi *tree* adalah hasil penggabungan dari topologi *bus* dan topologi *star*. Topologi jaringan berbentuk *tree* pada umumnya dipakai untuk interkoneksi antara hirarki dengan pusat yang berbeda-beda. Jenis topologi jaringan ini memiliki karakteristik khusus, yaitu adanya kabel utama sebagai penghubung beberapa *hub* pada jaringan *star*, memiliki hierarki, dan memiliki *hub* sebagai *server* pusat yang mengatur arus data.

6. Topologi *Mesh*

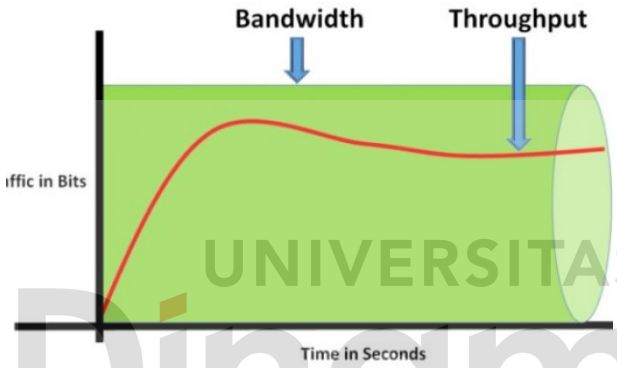


Gambar 10 Topologi *Mesh*

Topologi jaringan *mesh* (jala) adalah suatu topologi jaringan dimana setiap perangkat komputer saling terhubung secara langsung (*dedicated link*).

Topologi *mesh* biasanya digunakan untuk rute yang banyak dengan menggunakan kabel tunggal sehingga proses pengiriman data menjadi lebih cepat tanpa melalui *hub* atau *switch*. Jenis topologi jaringan komputer ini biasanya digunakan pada jaringan yang memiliki perangkat komputer sedikit. Pada topologi ini, koneksi antar komputer terhubung secara langsung sehingga meningkatkan kecepatan proses transfer data karena tidak ada perantara.

3.3 *Bandwidth* Internet

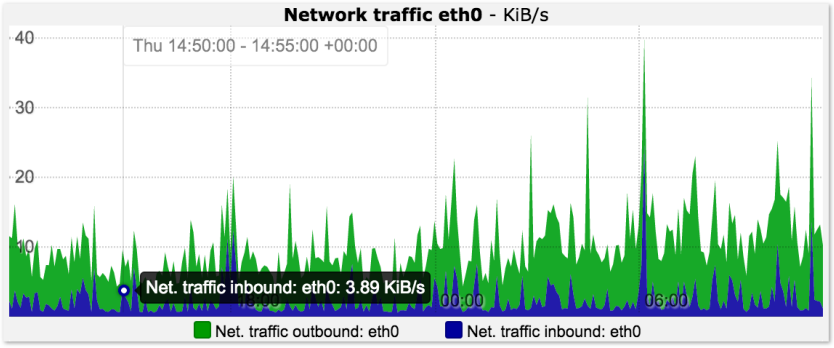


Gambar 11 Illustrasi *Bandwidth*

Bandwidth internet merupakan kapasitas maksimal jalur komunikasi untuk melakukan proses pengiriman dan penerimaan data dalam hitungan detik yang dihitung dalam satuan waktu *bit per second* (bps). *Bandwidth* sering dianalogikan dengan lebar jalan raya. Sedangkan data yang masuk melewati *bandwidth* diibaratkan kendaraan yang melintasi jalan tersebut. Semakin sedikit kendaraan yang lewat maka lalu lintas akan semakin lancar. Kebalikannya, jika kendaraan yang lewat banyak maka lalu lintas di jalan tersebut akan tersendat sehingga akan mempengaruhi aktivitas kendaraan lain. Semakin besar jalan *(bandwidth)* maka akan semakin banyak pula kendaraan yang dapat melaluinya. Maka tidak salah jika *bandwidth* menjadi pertimbangan pengguna jaringan internet. Dikarenakan

semakin besar *bandwidth* maka semakin cepat pertukaran data yang terjadi dan semakin banyak data yang dapat melaluinya dalam satu waktu.

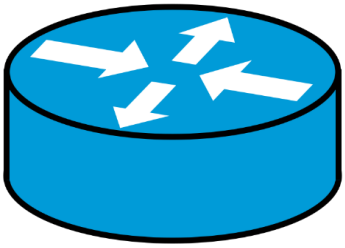
3.4 Lalu lintas Jaringan *(Network Traffic)*



Gambar 12 Illustrasi *traffic* jaringan

Lalu lintas jaringan atau lalu lintas data adalah jumlah data yang bergerak melintasi jaringan pada suatu titik waktu tertentu. Data jaringan dalam jaringan komputer sebagian besar dikemas dalam bentuk paket jaringan, sehingga dapat memberikan beban dalam jaringan. Lalu lintas jaringan adalah komponen atau variabel utama untuk melakukan pengukuran lalu lintas jaringan, pengendalian lalu lintas jaringan dan simulasi.

3.5 *Router*



Gambar 13 Simbol *router*

Router adalah sebuah alat yang mengirimkan paket data atau informasi melalui sebuah jaringan atau internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai *routing*. *Router* berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya, artinya *router* secara cerdas dapat mengetahui kemana rute perjalanan informasi atau paket akan dilewatkan, apakah ditujukan untuk *host* lain yang satu *network* ataukah berada di *network* yang berbeda. Jika informasi atau paket ditujukan untuk *host* pada *network* lain maka *router* akan meneruskannya ke *network* tersebut. Sebaliknya, jika informasi atau paket ditujukan untuk *host* yang satu *network* maka *router* akan menghalangi informasi atau paket tersebut keluar.

3.6 MikroTik

Gambar 14 Perangkat MikroTik

MikroTik merupakan sebuah perangkat keras yang berfungsi sebagai network *router*. Didalam MikroTik, terdapat RouterOS yang disebut dengan MikroTik RouterOS, MikroTik RouterOS sendiri adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer biasa menjadi *router network* yang handal, mencakup berbagai fitur yang dibuat untuk *IP network* dan jaringan *wireless*. Fitur-fitur tersebut diantaranya: *Firewall NAT,*

Routing, Hotspot, Point to Point Tunneling Protocol, DNS server, DHCP server, dan masih banyak lagi fitur lainnya.

MikroTik RouterOS merupakan sistem operasi berbasis *Linux* yang diperuntukkan sebagai *network router*. Didesain untuk memberikan kemudahan bagi penggunanya. Administrasi dan proses konfigurasinya bisa dilakukan melalui *Windows Application* yang sering disebut dengan aplikasi *WinBox.*

3.7 WinBox

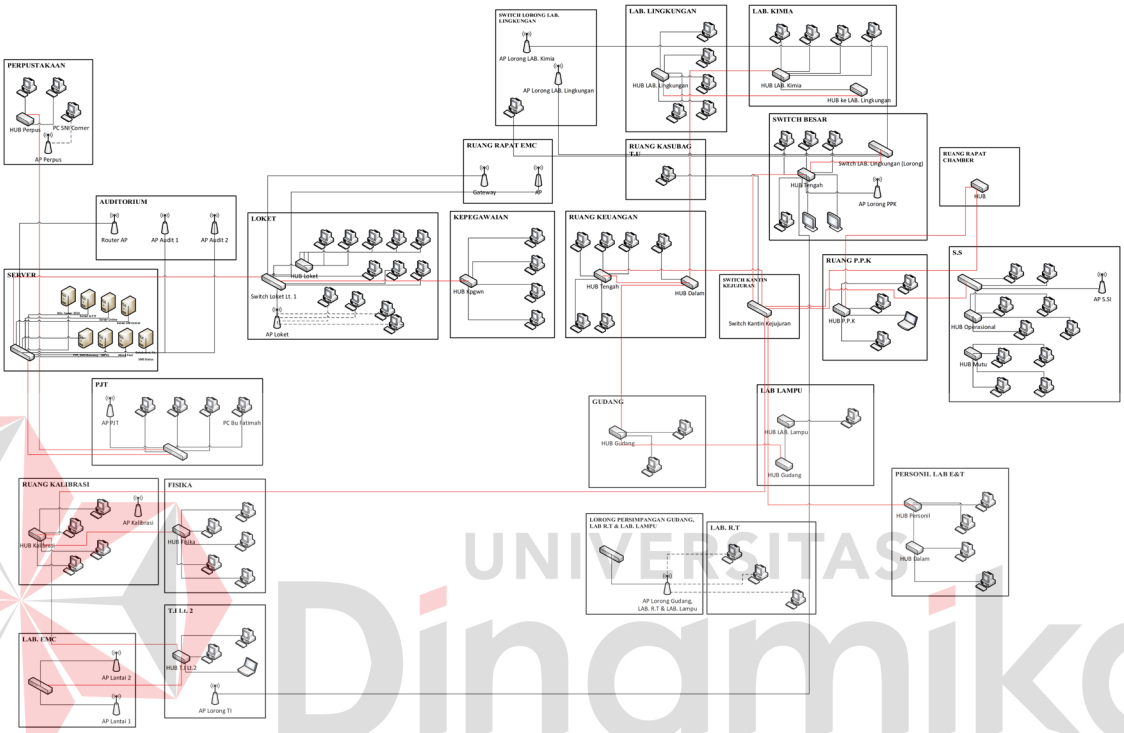
Gambar 15 Logo WinBox

WinBox adalah salah satu aplikasi untuk konfigurasi MikroTik RouterOS menggunakan *Graphical User Interface (GUI)*. Aplikasi WinBox bisa berjalan pada windows berbentuk *portable binary*, tapi bisa juga berjalan pada *Linux* dan *MACOS (OSX)* menggunakan *Wine*. Semua fungsi pada aplikasi WinBox hampir sama persis dengan fungsi konsol *(command line).*

BAB IV

DESKRIPSI PEKERJAAN

4.1 Topologi Jaringan BARISTAND Industri Surabaya



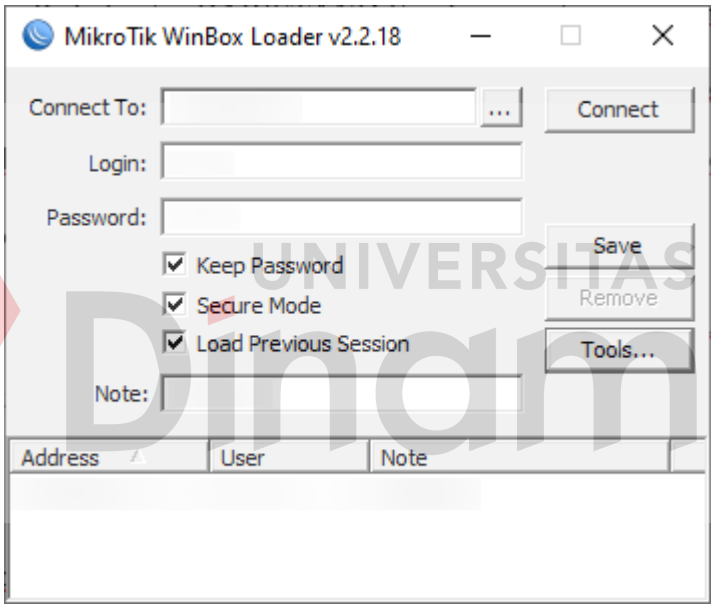
Gambar 16 Topologi jaringan

Pada gambar 16 menunjukkan alur dari penataan kabel dan penempatan perangkatnya, jaringan tersebut berfungsi untuk menyambungkan koneksi internet ke setiap perangkat yang ada di kantor BARISTAND Industri Surabaya. Sehingga setiap perangkat yang terhubung ke internet dapat mengakses secara *online* maupun *offline* (karena masih dalam satu jaringan lokal) ke *server* yang ada di kantor BARISTAND Industri Surabaya. Selain itu, dengan topologi tersebut memungkinkan setiap perangkat dapat berkomunikasi secara lokal sehingga dapat melakukan aktifitas *sharing* dengan perangkat lainnya, seperti *file sharing, printer sharing,* dan *scan sharing*.

4.2 Mengakses *Router* MikroTik

Pada kantor BARISTAND Industri Surabaya saat ini menggunakan MikroTik RB11004AhX yang befungsi sebagai *router* untuk mengakomodir semua kegiatan *routing* yang diperlukan. Untuk dapat mengkases *router*, ada beberapa cara yang dapat digunakan diantaranya yaitu : *ssh, telnet, web base service,* dan dengan aplikasi WinBox.

Dalam laporan ini, penulis akan menggunakan aplikasi WinBox untuk mengakses *router* yang ada di kantor BARISTAND Industri Surabaya.



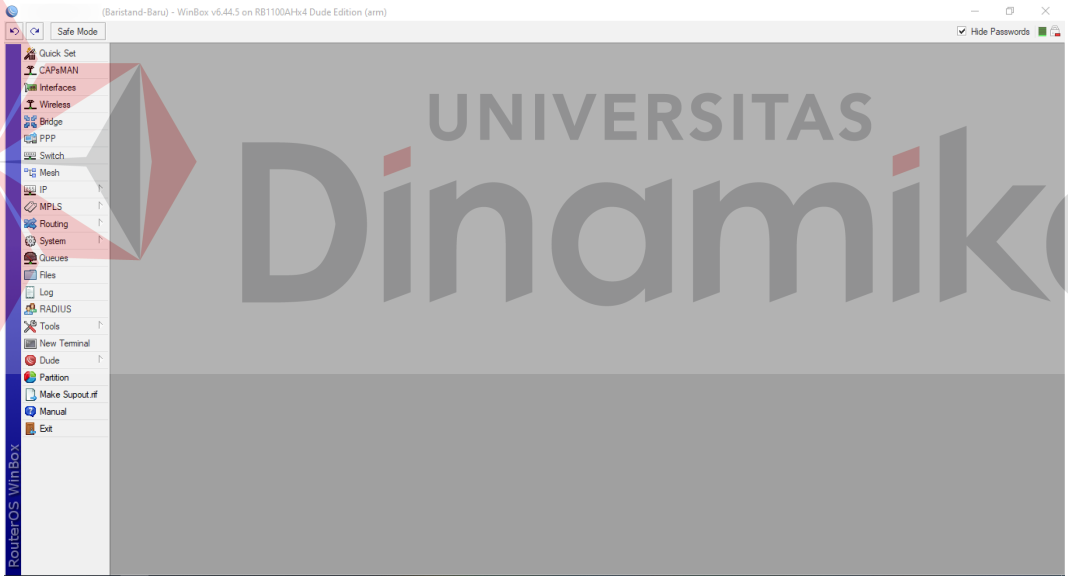
Gambar 17 Tampilan awal WinBox

Berikut penjelasannya :

1. *Connect To :* Untuk menghubungkan ke *router* yang akan diakses, bisa diisi dengan IP *router* tujuan atau dengan *MAC Address* dari *router* apabila berada di jaringan lokal.
2. Tombol *Connect :* Untuk melakukan koneksi ke IP *router* tujuan.
3. *Login :* Kolom untuk memasukkan *Username.*

4. *Password :* Kolom untuk memasukkan *Password.*
5. Tombol *Save :* Untuk mengelola dan menyimpan alamat *IP* atau *MAC Address* dari *router* yang sudah di konfigurasi sebelumnya.
6. *Note :* Untuk memberi catatan ketika akan menyimpan sesi *login.*

Setelah memasukkan *username* dan *password* yang penulis miliki, selanjutnya klik tombol *Connect,* maka akan tampil *progress bar* yang menunjukkan proses *login* sedang berlangsung, setelah selesai maka akan tampil *interface* dari *router* yang dapat dikonfigurasi oleh *user seperti pada gambar 18.* Untuk konfigurasinya bisa disesuaikan dengan kebutuhan, sehingga tidak semua fitur yang ada di *router* akan terpakai.



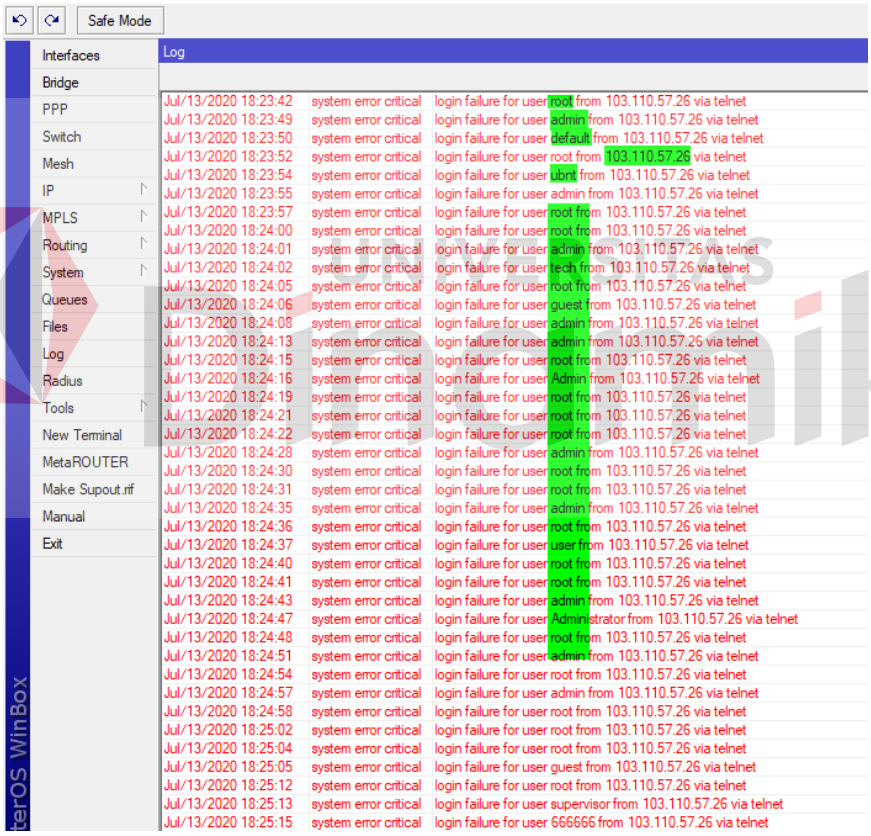
Gambar 18 Tampilan setelah *user login*

4.3 Mengamankan *Router*

Dalam melakukan konfigurasi *router* MikroTik pada jaringan yang kita miliki, hal yang sangat penting dan perlu diperhatikan adalah mengenai keamanan

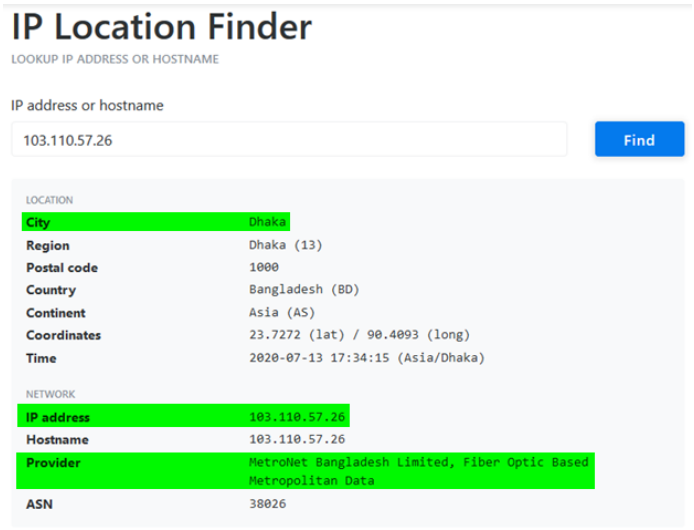
router. Sebagai admin jaringan, jangan sampai lupa untuk melakukan proteksi atau mengamankan *router* dari pihak-pihak luar yang tidak bertanggung jawab.

Seperti yang sebelumnya terjadi pada *router* di kantor BARISTAND Industri Surabaya yang mengalami serangan jenis *Brute Force Attack* yaitu serangan yang berupaya untuk mendapatkan akses ke *router* dengan cara menggunakan algoritma yang menggabungkan huruf, angka dan simbol untuk menghasilkan *username* dan *password* yang sebelumnya sudah tercatat di *wordlist* dalam jumlah yang banyak untuk menebak kemungkinan *username* dan *password.*



Gambar 19 Serangan *Brute Force Attack* pada router

Dari tampilan *log* diatas, admin jaringan dapat melakukan pelacakan ke alamat *IP* penyerang, yaitu *IP 103.110.57.26* agar tahu asal dari alamat *IP* tersebut.



Gambar 20 Hasil Penelusuran Alamat *IP* 103.110.57.26

Setelah dilakukan penelusuran dengan menggunakan bantuan website https://tools.keycdn.com/geo, maka diketahui bahwa alamat *IP* tersebut berasal dari Bangladesh dan dimiliki oleh salah satu vendor penyedia jasa internet dengan nama Metronet Bangladesh Limited. Untuk menghindari serangan tersebut terulang kembali, maka perlu dilakukan pengamanan terhadap *router* yang ada. Langkah-langkah yang perlu dilakukan untuk mengamankan *router* MikroTik sebagai berikut :

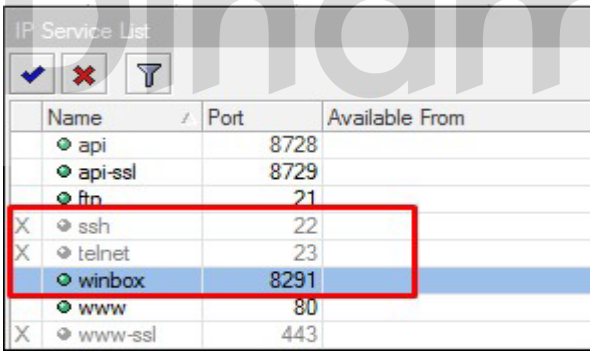
1. Mengubah *username* dan *password router*

   Sudah bukan rahasia lagi kalau *router* MikroTik mempunyai *username* dan *password* bawaan pabrik yaitu *username* : Admin, dan *password* : (kosong). Sebaiknya *username* dan *password default* tersebut dihapus atau diubah, agar tidak digunakan orang lain. Untuk menghapus dan melakukan *disable user default* silakan buat terlebih dahulu *user* yang memiliki hak akses (group) *full*. Untuk melakukan *management user* bisa masuk ke menu ***System > Users***.

Gambar 21 Tampilan menu *User List*

2. Mengubah atau mematikan *service* yang tidak diperlukan

   Service di *router* secara *default* sudah terbuka, jadi admin jaringan harus mengantisipasi beberapa *service* yang digunakan untuk melakukan *remote* akses ke *router*. Dengan cara menonaktifkan *service* tersebut, mengubah *port* defaultnya atau membatasi hanya beberapa alamat *IP* saja yang boleh akses menggunakan *port* tersebut. Pengaturan ini dapat dilakukan pada menu ***IP > Services***.



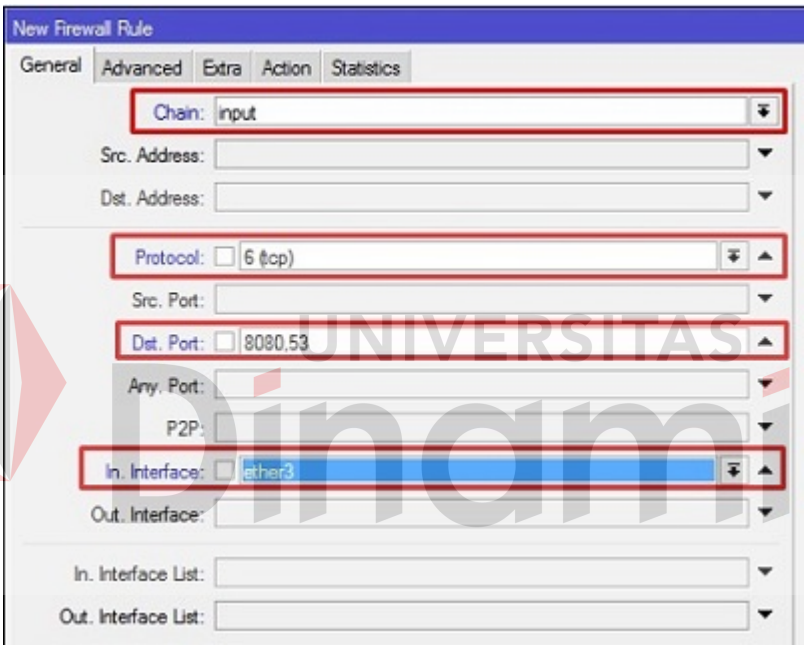
Gambar 22 Tampilan menu *IP Service List*

3. Mengaktifkan *firewall filter* untuk akses *Domain Name Server (DNS)* dan *Web Proxy*

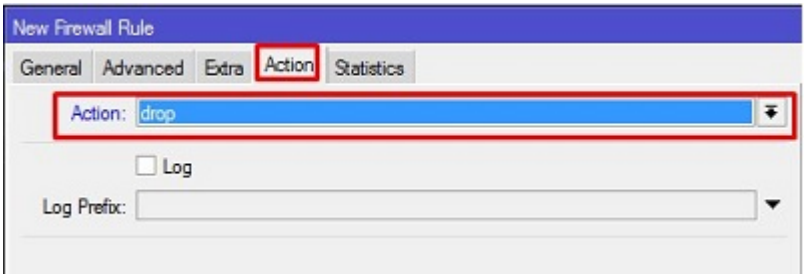
   Router MikroTik yang diposisikan sebagai *gateway* utama, sering mengaktifkan fitur *Allow-remote-request DNS* dan *web proxy*. Kedua fitur tersebut bisa dimanfaatkan oleh pihak luar terutama *web proxy* yang kadang

membuat trafik internasional sering penuh padahal tidak ada *user* lokal yang menggunakannya.

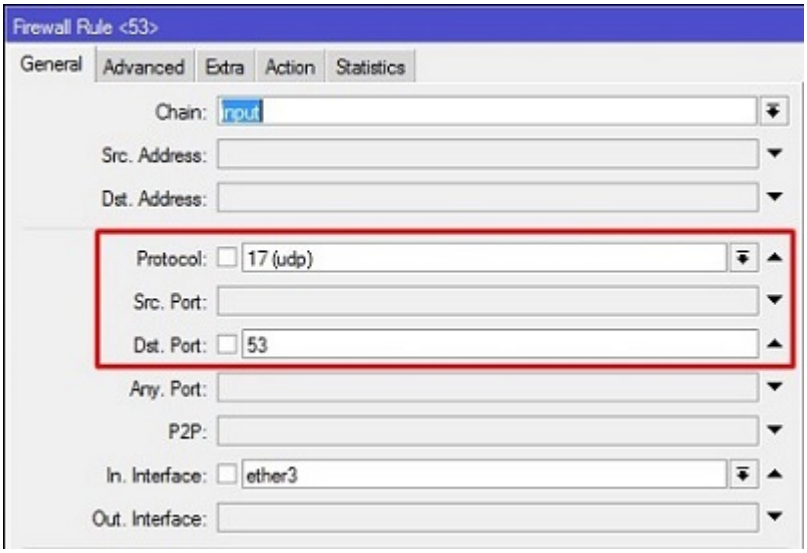
Untuk mengatasi hal tersebut admin jaringan harus mengaktifkan *filter* pada *firewall* agar pihak luar tidak bisa memanfaatkan *DNS* dan *Web Proxy* dari jaringan yang dimiliki BARISTAND Industri Surabaya. Berikut cara yang bisa dilakukan dengan menggunakan WinBox untuk mengakses *router,* yaitu melalui menu ***IP > Firewall > Filter Rules***.



Gambar 23 Konfigurasi *firewall* pada tab *General* untuk *port TCP*



Gambar 24 Konfigurasi *firewall filter* pada tab *Action*



Gambar 25 Konfigurasi *firewall* pada tab *General* untuk *port UDP*

Setelah melakukan semua konfigurasi diatas, pastikan kembali pada menu ***IP > Firewall > Filter Rules*** sudah ada konfigurasi baru yang sudah ditambahkan.

4.4 Pembagian Jumlah *Host* dengan *IP Address Subnet* /23

IP address adalah sebuah alamat pada komputer agar bisa saling terhubung dengan komputer lain, *IP address* terdiri dari 4 Blok, setiap blok diisi oleh angka 0 – 255. Contoh *IP address* seperti 192.168.100.1, 10.57.38.223 , ini adalah IPv4. *IP address* memiliki 2 bagian, yaitu *network ID* dan h*ost ID*, contoh 192.168.100.1, secara *default, network ID*nya adalah 192.168.100 dan *host ID*nya adalah 1, agar komputer bisa saling terhubung, *IP* yang digunakan *network ID*nya harus sama, dan *host ID*nya harus berbeda.

Pada BARISTAND Industri Surabaya, *IP* yang dipakai adalah *IP* kelas C yang berarti 4 bit pertama adalah *network ID*, dan 8 bit selanjutnya adalah *host ID*, kelas C memiliki *network ID* dari 192 sampai 223. Dan *prefix* yang digunakan

adalah /23 yang berarti jumlah maksimal perangkat yang dapat terhubung ke internet sebanyak 512 perangkat.

Subnet Mask Quick Reference							
CIDR	Host Bit Length	Math	Max Hosts	Subnet Mask	Mask Octet	Binary Mask	Subnet Length
/32	0	2^0	1	255.255.255.255	4	11111111	0
/31	1	2^1	2	255.255.255.254	4	11111110	1
/30	2	2^2	4	255.255.255.252	4	11111100	2
/29	3	2^3	8	255.255.255.248	4	11111000	3
/28	4	2^4	16	255.255.255.240	4	11110000	4
/27	5	2^5	32	255.255.255.224	4	11100000	5
/26	6	2^6	64	255.255.255.192	4	11000000	6
/25	7	2^7	128	255.255.255.128	4	10000000	7
/24	8	2^8	256	255.255.255.0	3	11111111	8
Kelas C							
/23	9	2^9	512	255.255.254.0	3	11111110	9
/22	10	2^10	1,024	255.255.252.0	3	11111100	10
/21	11	2^11	2,048	255.255.248.0	3	11111000	11
/20	12	2^12	4,096	255.255.240.0	3	11110000	12
/19	13	2^13	8,192	255.255.224.0	3	11100000	13
/18	14	2^14	16,384	255.255.192.0	3	11000000	14
/17	15	2^15	32,768	255.255.128.0	3	10000000	15
/16	16	2^16	65,536	255.255.0.0	2	11111111	16
Kelas B							
/15	17	2^17	131,072	255.254.0.0	2	11111110	17
/14	18	2^18	262,144	255.252.0.0	2	11111100	18
/13	19	2^19	524,288	255.248.0.0	2	11111000	19
/12	20	2^20	1,048,576	255.240.0.0	2	11110000	20
/11	21	2^21	2,097,152	255.224.0.0	2	11100000	21
/10	22	2^22	4,194,304	255.192.0.0	2	11000000	22
/9	23	2^23	8,388,608	255.128.0.0	2	10000000	23
/8	24	2^24	16,777,216	255.0.0.0	1	11111111	24
Kelas A							

Gambar 26 Pembagian *IP address* beserta jumlah maksimal pengguna

4.5 Pembagian *Bandwidth*

Pada sebuah jaringan yang mempunyai banyak pengguna atau *client*, diperlukan sebuah mekanisme pengaturan *bandwidth* dengan tujuan mencegah terjadinya monopoli penggunaan *bandwidth* sehingga semua pengguna bisa mendapatkan jatah *bandwidth* masing-masing. *QoS (Quality of Services)* atau lebih dikenal dengan *bandwidth management*, merupakan metode yang digunakan untuk memenuhi kebutuhan tersebut. Pada MikroTik penerapan *QoS* bisa dilakukan dengan fungsi *Queue*.

Cara paling mudah untuk melakukan *queue* di MikroTik adalah dengan menggunakan *Simple Queue*. Pada kantor BARISTAND Industri Surabaya saat ini diterapkan metode pembagian *bandwidth share* yaitu penerapan limitasi bertingkat.

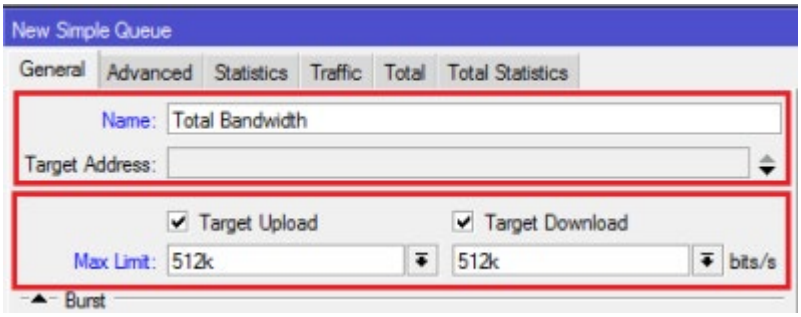
Konsep :

Dalam percobaan ini akan dilakukan pengaturan *bandwidth* sebesar 512kbps untuk digunakan 3 *client*.

Konsep :

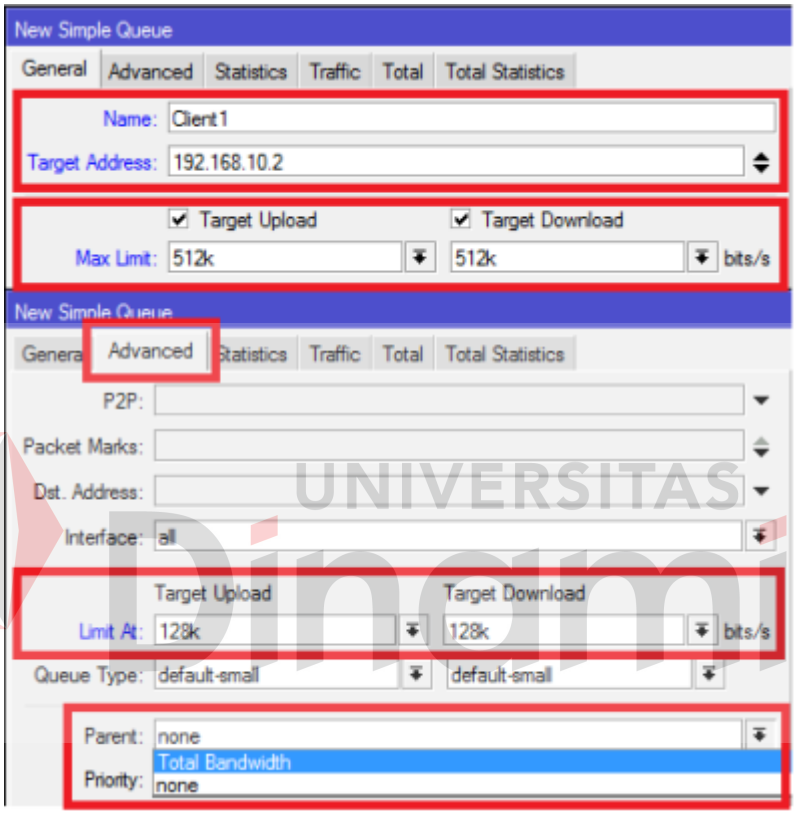
1. Dalam keadaan semua *client* melakukan akses internet, maka masing-masing *client* akan mendapat *bandwidth* minimal 128kbps.
2. Jika hanya ada 1 *client* yang melakukan akses internet, maka *client* tersebut bisa mendapatkan *bandwidth* hingga 512kbps.
3. Jika terdapat beberapa Client (tidak semua client) melakukan akses, maka *bandwidth* yang tersedia akan dibagi rata ke sejumlah client yang aktif.

Router tidak tahu berapa total *bandwidth* asli yang dimiliki, maka admin jaringan harus definisikan pada langkah pertama. Pendefinisian ini bisa dilakukan dengan melakukan konfigurasi *queue parent*. Besar *bandwidth* yang dimiliki bisa diisikan pada parameter *Target Upload Max-Limit* dan *Target Download Max-Limit.*



Gambar 27 Pendefinisian total *bandwidth* yang dimiliki

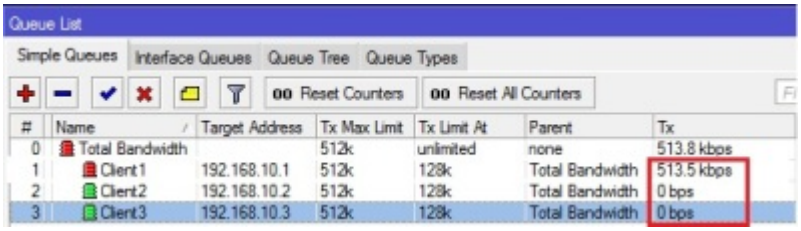
Langkah selanjutnya, admin jaringan perlu menentukan batas kecepatan untuk setiap *client* dengan melakukan konfigurasi *child-queue.* Pada *child-queue* admin jaringan mulai mentukan *target-address* dengan mengisikan *IP address* masing-masing *client*. Terapkan *Limit-at (CIR)* : 128kbps dan *Max-Limit (MIR)* : 512kbps. Arahkan ke *Parent Total Bandwidth* yang sudah buat sebelumnya.



Gambar 28 Konfigurasi pembagian *bandwidth* untuk tiap *client*

Selanjutnya lakukan pengetesan sebanyak 3 kali dengan melakukan *download* di sisi *client* dengan 3 kondisi, yaitu percobaan pertama hanya akan ada 1 *client* yang aktif mengakses internet. Percobaan kedua akan ada 2 *client* yang akan mengakses internet secara bersamaan, dan percobaan ketiga akan dilakukan dengan menambahkan 1 *client* sehingga menjadi 3 *client* yang akan mengakses internet secara bersamaan.

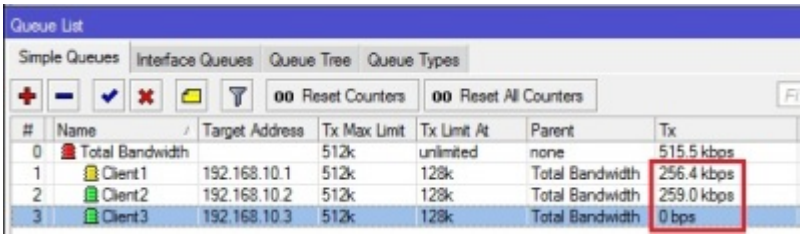
Kondisi 1 menunjukkan ketika hanya 1 *client* yang sedang mengakses internet, maka *client* tersebut bisa mendapat kecepatan internet hingga *max-limit*. Perhitungan: Pertama *router* akan memenuhi *Limit-at client* yaitu 128kbps. *Bandwitdh* yang tersedia masih sisa 512kbps - 128kbps = 384kbps. Karena *client* yang lain tidak aktif maka 384kbps yang tersisa akan diberikan lagi ke *client 1* sehingga mendapat 128kbps + 384kbps = 512kbps atau sama dengan *max-limit*.



Gambar 29 Hasil percobaan penggunaan *bandwidth* dengan 1 *client*

Kondisi 2 menggambarkan ketika hanya 2 *client* yang sedang mengakses internet, maka *bandwidth* secara otomatis akan dibagi untuk kedua *client* tersebut.

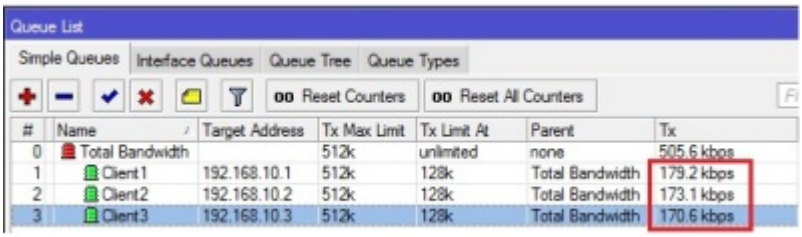
Perhitungan: Pertama *router* akan memberikan *limit-at* semua *client* terlebih dahulu. Akumulasi *limit-at* untuk 2 client = 128kbps * 2 = 256kbps . *Bandwidth* total masih tersisa 256kbps, dari sisa bagi tersebut maka *bandwidth* akan dibagi rata ke kedua *client* yang terhubung. Sehingga tiap *client* akan mendapat kecepatan sebesar 256kbps, yang didapat dari penjumlahan antara *limit-at* dengan total *bandwidth* yaitu 128kbps + 128kbps =256kbps.



Gambar 30 Hasil percobaan penggunaan *bandwidth* dengan 2 *client*

Kondisi 3 diasumsikan bahwa semua *client* sedang mengakses internet sehingga memerlukan *bandwidth*.

Perhitungan: Pertama *router* akan memenuhi *limit-at* tiap *client* lebih dulu, sehingga *bandwidth* yang digunakan 128kbps x 3 = 384kbps. *Bandwidth* total masih tersisa 128kbps. Sisa *bandwidth* akan dibagikan ke ketiga *client* secara merata sehingga tiap *client* mendapat 128kbps + (128kbps/3) = 170kbps.



Gambar 31 Hasil percobaan penggunaan *bandwidth* dengan 3 *client*

Dengan metode ini maka penggunaan *bandwidth* yang ada di kantor BARISTAND Industri Surabaya akan lebih efektif dan efisien sehingga tidak akan mengganggu pengguna atau *client* lainnya yang juga sama-sama sedang mengakses internet.

4.6 Implementasi *Bandwidth* Priority Video Conference aplikasi Zoom

Untuk meciptakan rasa nyaman ketika menggunakan internet di kantor, maka dalam kesempatan ini akan dicoba untuk mengoptimalkan jaringan dengan memprioritaskan koneksi yang digunakan *video conference* agar bisa digunakan dengan baik tanpa ada gangguan. *Bandwidth* yang digunakan akan diprioritaskan agar tidak terganggu saat ada *client* lain sedang melakukan *browsing* ke internet.

Sebelumnya, perlu dicari terlebih dahulu semua informasi mengenai aplikasi *Zoom*, baik dari *ip server*, protokol dan *port* yang digunakan. Informasi

dari website resmi *Zoom*, aplikasi *Zoom* menggunakan protokol *TCP* dan *UDP* dengan *port* 80, 443, 3478, 3479, 5090, 5091, 8801-8810. Protokol dan *port* tersebut yang akan digunakan untuk menangkap *traffic* menuju *server Zoom*. Selain protokol dan *port*, bisa juga berdasarkan *IP server Zoom* yang akan ditambahkan ke dalam *router*.

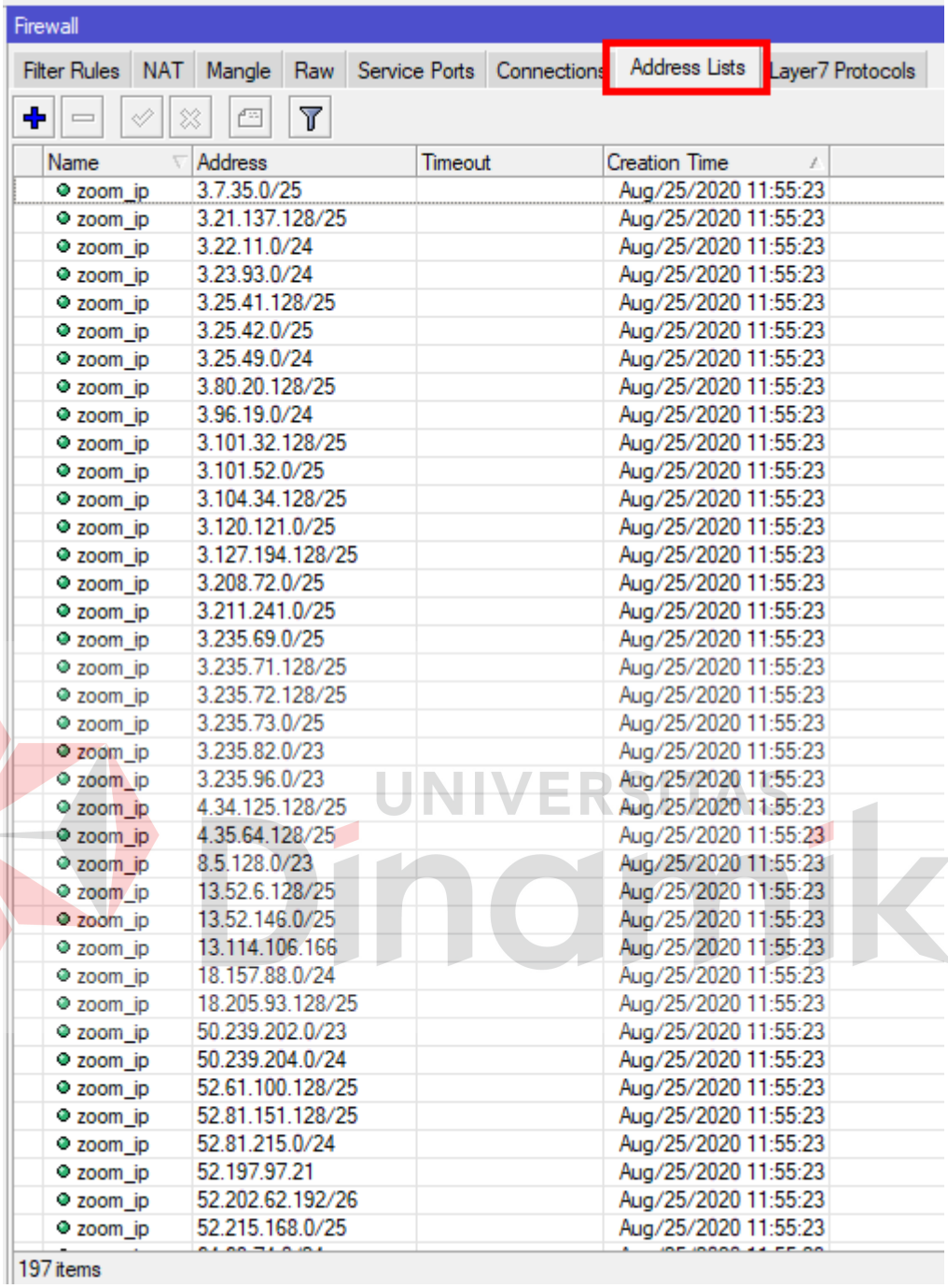
Langkah pertama, menambahkan List *IP server Zoom* menggunakan *script* berikut ini, dengan cara membuka *New Terminal* lalu mengetikkan *script* yang tertera.

Tabel 1 *Script list IP server Zoom*

```
/ip firewall address-list
add address=3.7.35.0/25 list=zoom_ip
add address=3.21.137.128/25 list=zoom_ip
add address=3.22.11.0/24 list=zoom_ip
add address=3.23.93.0/24 list=zoom_ip
add address=3.25.41.128/25 list=zoom_ip
add address=3.25.42.0/25 list=zoom_ip
add address=3.25.49.0/24 list=zoom_ip
add address=3.80.20.128/25 list=zoom_ip
add address=3.96.19.0/24 list=zoom_ip
add address=3.101.32.128/25 list=zoom_ip
add address=3.101.52.0/25 list=zoom_ip
add address=3.104.34.128/25 list=zoom_ip
add address=3.120.121.0/25 list=zoom_ip
add address=3.127.194.128/25 list=zoom_ip
add address=3.208.72.0/25 list=zoom_ip
add address=3.211.241.0/25 list=zoom_ip
add address=3.235.69.0/25 list=zoom_ip
add address=3.235.82.0/23 list=zoom_ip
add address=3.235.71.128/25 list=zoom_ip
add address=3.235.72.128/25 list=zoom_ip
add address=3.235.73.0/25 list=zoom_ip
add address=3.235.96.0/23 list=zoom_ip
add address=4.34.125.128/25 list=zoom_ip
add address=4.35.64.128/25 list=zoom_ip
add address=8.5.128.0/23 list=zoom_ip
add address=13.52.6.128/25 list=zoom_ip
add address=13.52.146.0/25 list=zoom_ip
add address=13.114.106.166 list=zoom_ip
add address=18.157.88.0/24 list=zoom_ip
add address=18.205.93.128/25 list=zoom_ip
```

```
add address=50.239.202.0/23 list=zoom_ip
add address=50.239.204.0/24 list=zoom_ip
add address=52.61.100.128/25 list=zoom_ip
add address=52.81.151.128/25 list=zoom_ip
add address=52.81.215.0/24 list=zoom_ip
add address=52.197.97.21 list=zoom_ip
add address=52.202.62.192/26 list=zoom_ip
add address=52.215.168.0/25 list=zoom_ip
add address=64.69.74.0/24 list=zoom_ip
add address=64.125.62.0/24 list=zoom_ip
add address=64.211.144.0/24 list=zoom_ip
add address=65.39.152.0/24 list=zoom_ip
add address=69.174.57.0/24 list=zoom_ip
add address=69.174.108.0/22 list=zoom_ip
add address=99.79.20.0/25 list=zoom_ip
add address=103.122.166.0/23 list=zoom_ip
add address=109.94.160.0/22 list=zoom_ip
add address=109.244.18.0/25 list=zoom_ip
add address=109.244.19.0/24 list=zoom_ip
add address=111.33.181.0/25 list=zoom_ip
add address=115.110.154.192/26 list=zoom_ip
add address=115.114.56.192/26 list=zoom_ip
add address=115.114.115.0/26 list=zoom_ip
add address=115.114.131.0/26 list=zoom_ip
add address=120.29.148.0/24 list=zoom_ip
add address=140.238.128.0/24 list=zoom_ip
add address=147.124.96.0/19 list=zoom_ip
add address=149.137.0.0/17 list=zoom_ip
```

Jika sudah berhasil, cek ulang pada menu ***IP > Firewall > Address Lists*** apakah *IP Zoom* sudah tertambahkan secara otomatis dan akan ada list *IP server Zoom* dengan nama "**zoom_ip"**.



Gambar 32 *IP Server Zoom* setelah berhasil ditambahkan ke *Address Lists*

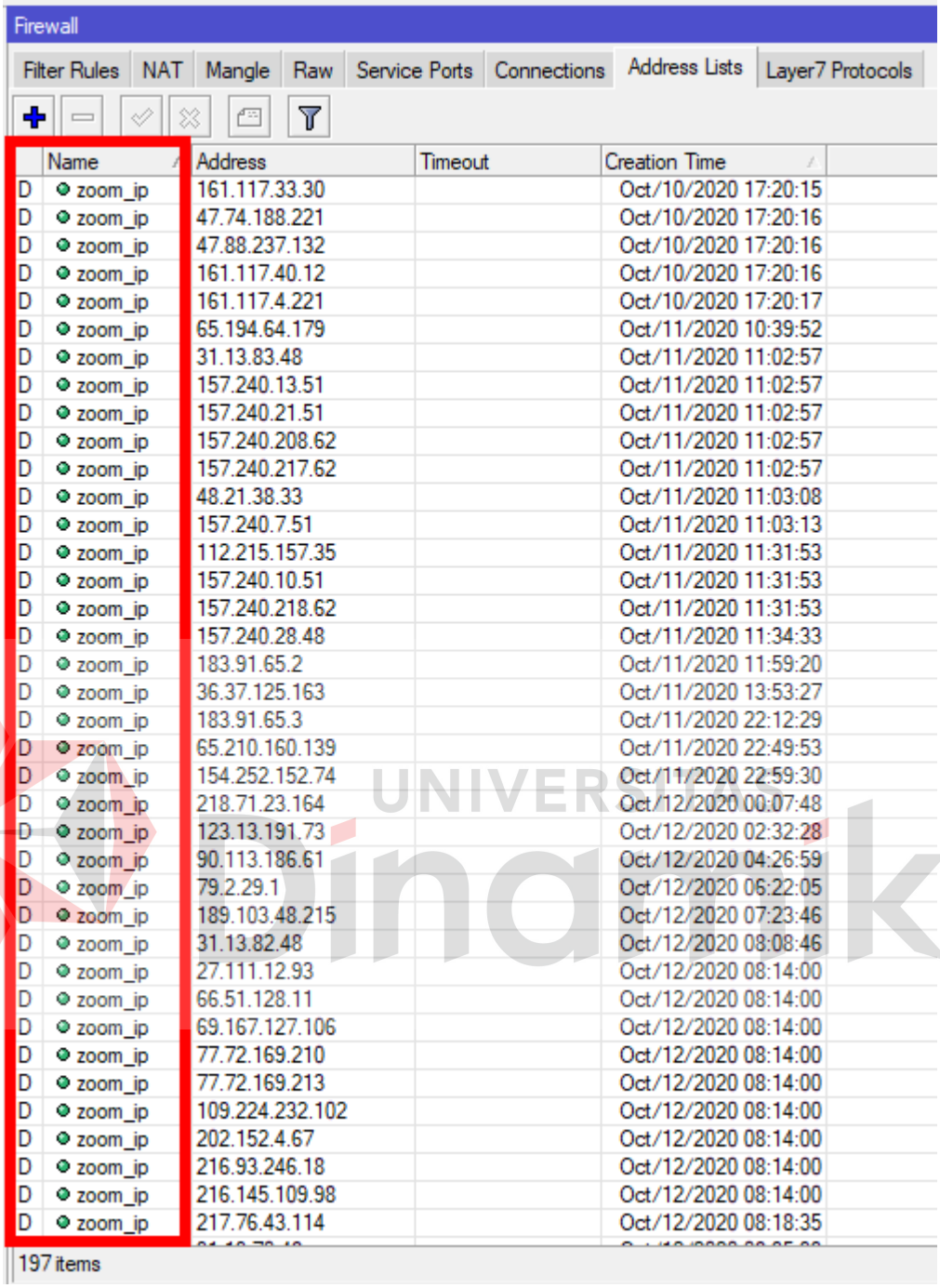
Perlu diketahui, tidak semua *IP* yang digunakan oleh *server Zoom* ada pada *script* tersebut. Untuk menambahkan secara otomatis, tambahkan *rule mangle* berdasarkan *port* yang digunakan oleh aplikasi *Zoom*. Menambahkan dua

rule untuk *TCP* dan *UDP* dengan *destination port* yaitu port **3478, 3479, 5090, 5091, 8801-8810** (selain **80** dan **443**). Berikut *script* yang digunakan :

Tabel 2 *Script rule TCP* dan *UDP*

```
/ip firewall mangle
add chain=prerouting dst-address-list=!zoom  ip dst-port=3478,3479,5090,5091,8801-8810 protocol=tcp action=add-dst-to-address-list address-list=zoom_ip;
add chain=prerouting dst-address-list=!zoom  ip dst-port=3478,3479,5090,5091,8801-8810 protocol=udp action=add-dst-to-address-list address-list=zoom_ip;
```

Kedua *rule* diatas digunakan untuk menambahkan *IP* baru yang belum terdaftar pada *address-lists*. Nama *address-lists* nya dibuat sama dengan *list* import yaitu “zoom_ip” dan akan diperbaharui otomatis jika ada koneksi baru kearah *server Zoom*.



Gambar 33 *IP* dinamis dari *server Zoom*

Perbedaannya ditandai dengan adanya simbol **D** pada kolom sebelah kiri, yang menandakan bahwa *IP* tersebut bersifat dinamis. Langkah selanjutnya, untuk menangkap *traffic* koneksi aplikasi *Zoom*, perlu menambahkan *rule* baru pada *mangle* dengan *action mark-connection*. Protokol *port* diisi *port* yang digunakan

oleh *Zoom* yaitu Protokol *TCP* dan *UDP* dengan *port* 3478, 3479, 5090, 5091, 8801-8810. Kemudian memberi nama koneksi yang sudah ditangkap, contoh "koneksi_zoom" menggunakan *script* berikut ini.

Tabel 3 *Script* untuk *mark-connection traffic Zoom port* 3478

```
/ip firewall mangle
add chain=prerouting protocol=tcp dst-port=3478,3479,5090,5091,8801-8810
action=mark-connection new-connection-mark=koneksi  zoom passthrough=yes;
add  chain=prerouting  protocol=udp  dst-port=3478,3479,5090,5091,8801-8810
action=mark-connection new-connection-mark=koneksi_zoom passthrough=yes;
```

Selain *port* 3478, 3479, 5090, 5091, 8801-8810, aplikasi *Zoom* juga menggunakan protokol *TCP* 80 dan *TCP* 443. Menambahkan *rule* baru dengan *dst-port=80,443* dan *Dst. Address List = zoom_ip* yang sudah ditambahkan sebelumnya menggunakan *script* berikut ini.

Tabel 4 *Script* untuk *mark-connection traffic Zoom port* 80 dan 443

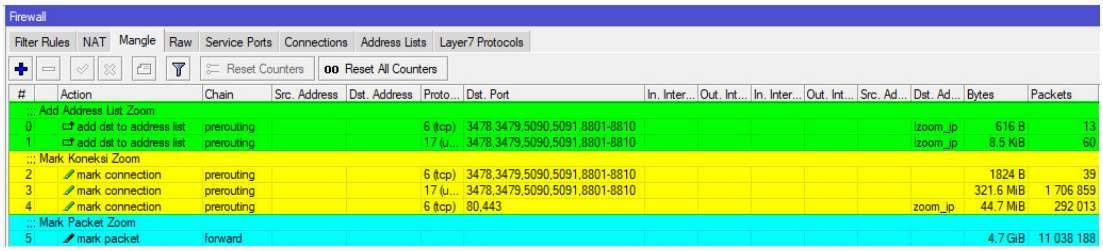
```
/ip firewall mangle add chain=prerouting protocol=tcp dst-port=80,443 dst-
address-list=zoom  ip action=mark-connection new-connection-
mark=koneksi_zoom passthrough=yes
```

Selanjutnya perlu melakukan *dst-address-list=zoom-ip* agar paket *browsing* lain tidak tertangkap oleh *rule* ini. Pastikan nama *mark-connection* sama dengan *rule* sebelumnya yaitu “koneksi_zoom”. Setelah koneksi tertangkap, ada satu *rule* lagi yang harus ditambahkan *yaitu mark-packet*. Tambahkan *rule* baru dengan *Action Mark Packet* beri nama “packet_zoom”. Pastikan *connection mark* diisi *mark-connection = koneksi_zoom* yang sudah dibuat. *Packet-mark* ini yang akan digunakan untuk *bandwidth management*, baik pada menu *simple queue* atau pada *queue tree*. Berikut *script* yang digunakan :

Tabel 5 *Script mangle rule* untuk keperluan *bandwidth management*

```
/ip firewall mangle
add chain=forward action=mark-packet connection-mark=koneksi_zoom new-packet-mark=paket_zoom passthrough=no
```

Untuk memastikan hasilnya, bisa dicek melalui menu ***IP > Firewall > Mangle***. Apabila sudah benar maka tampilan yang ada pada tabel *mangle* akan tampak seperti pada gambar 34.



Gambar 34 Hasil akhir mangle bandwidth priority aplikasi Zoom

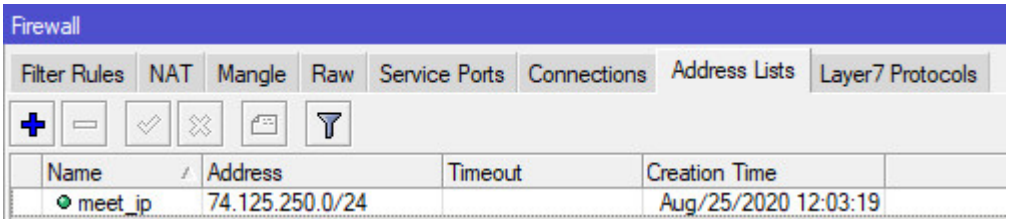
4.7 Implementasi *Bandwidth Priority Video Conference* Aplikasi *Google Meet*

Sama seperti sebelumnya, *server Google Meet* juga pasti memiliki beberapa *IP* yang berbeda. Untuk menambahkan *IP* tersebut, diperlukan *rule* baru agar *IP Google Meet* bisa ditangkap dan otomatis dimasukkan ke dalam *address-list*. Tambahkan dua *rule* untuk *TCP* dan *UDP* dengan *destination port* yaitu port **19302-19309** (selain **80** dan **443**). Berikut *script* yang digunakan :

Tabel 6 *Script* list *IP server Google Meet*

```
/ip firewall address-list
add address= 74.125.250.0/24 list=meet_ip;
```

Setelah selesai, dilanjtukan dengan memastikan bahwa *address-list* sudah tertambahkan secara otomatis melalui menu ***IP > Firewall > Address Lists***. Jika sudah benar maka akan tampak seperti gambar 35.



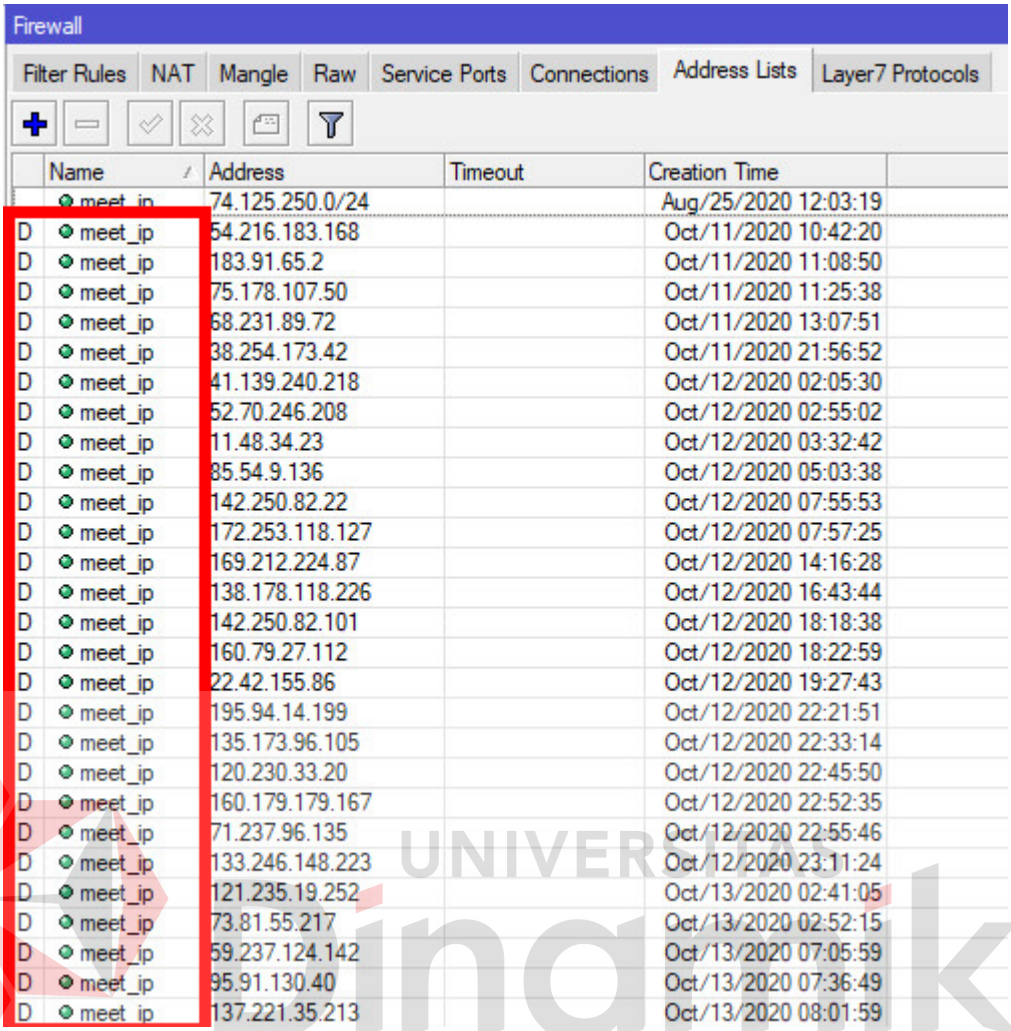
Gambar 35 IP statis Google Meet pada address list

Selanjutnya perlu dilakukan juga penambahan *rule* baru untuk menangkap *IP* dinamis dari *Google Meet* yang akan otomatis dimasukkan ke dalam *address-lists.* Tambahkan dua *rule* untuk *TCP* dan *UDP* dengan *destination port* yaitu port **19302-19309** (selain **80** dan **443**). Berikut *script* yang digunakan:

Tabel 7 *Script rule TCP* dan *UDP*

```
/ip firewall mangle
add chain=prerouting dst-address-list=!meet  ip dst-port=19302-19309
protocol=tcp action=add-dst-to-address-list address-list=meet  ip;
add  chain=prerouting  dst-address-list=!meet  ip  dst-port=19302-19309
protocol=udp action=add-dst-to-address-list address-list=meet_ip;
```

Pastikan bahwa tabel *address-lists* sudah bisa mengangkap *IP* dinamis dari *server Google Meet*, *IP* dinamis akan ditandai dengan adanya huruf **D** pada kolom pertama seperti gambar 36.



Gambar 36 IP dinamis dari server Google Meet

Langkah selanjutnya adalah membuat *mangle* untuk menangkap *traffic* koneksi *Google Meet* dengan menambahkan *action mark-connection*. Protokol *port* diisi *TCP* dan *UDP* dengan *port* 19302-19309. Beri nama "koneksi_meet".

Tabel 8 *Script* untuk *mark-connection traffic Google Meet port* 19302-19309

```
/ip firewall mangle
add chain=prerouting protocol=tcp dst-port=19302-19309 action=mark-
connection new-connection-mark=koneksi_meet passthrough=yes;
add chain=prerouting protocol=udp dst-port=19302-19309 action=mark-
connection new-connection-mark=koneksi_meet passthrough=yes;
```

Selain port 19302-19309, aplikasi *Google Meet* juga menggunakan protokol *TCP* 80 dan *TCP* 443. Tambahkan *rule* baru dengan *dst-port=80,443* dan

Dst. Address List = meet_ip yang sudah ditambahkan sebelumnya. Berikut *script* yang digunakan :

Tabel 9 *Script* untuk *mark-connection traffic Google Meet port* 19302-19309

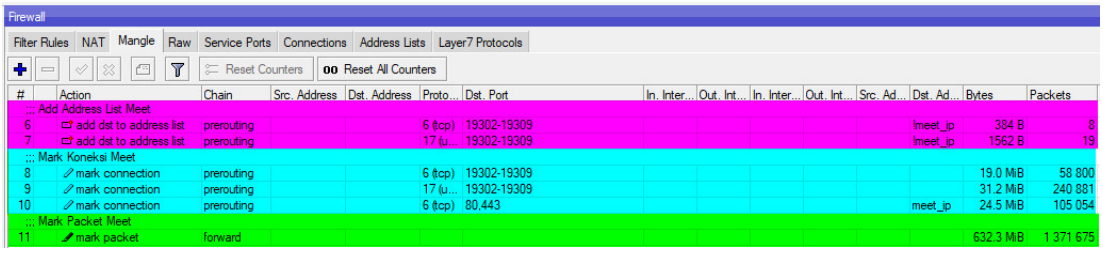
```
/ip firewall mangle
add chain=prerouting protocol=tcp dst-port=80,443 dst-address-list=meet_ip
action=mark-connection new-connection-mark=koneksi_meet passthrough=yes
```

Setelah koneksi tertangkap, ada satu *rule* lagi yang harus ditambahkan yaitu *mark-packet*. Tambahkan *rule* baru dengan *Action Mark Packet* beri nama "packet_meet". Pastikan *connection mark* diisi *mark-connection = koneksi_meet* yang sudah dibuat sebelumnya. Berikut *script* yang digunakan :

Tabel 10 *Script mangle rule* untuk keperluan *bandwidth management*

```
/ip firewall mangle
add chain=forward action=mark-packet connection-mark=koneksi_zoom new-
packet-mark=paket_zoom passthrough=no
```

Untuk memastikan hasilnya, bisa dicek melalui menu ***IP > Firewall > Mangle***. Apabila sudah benar maka tampilan yang ada pada tabel *mangle* akan tampak seperti pada gambar 37.

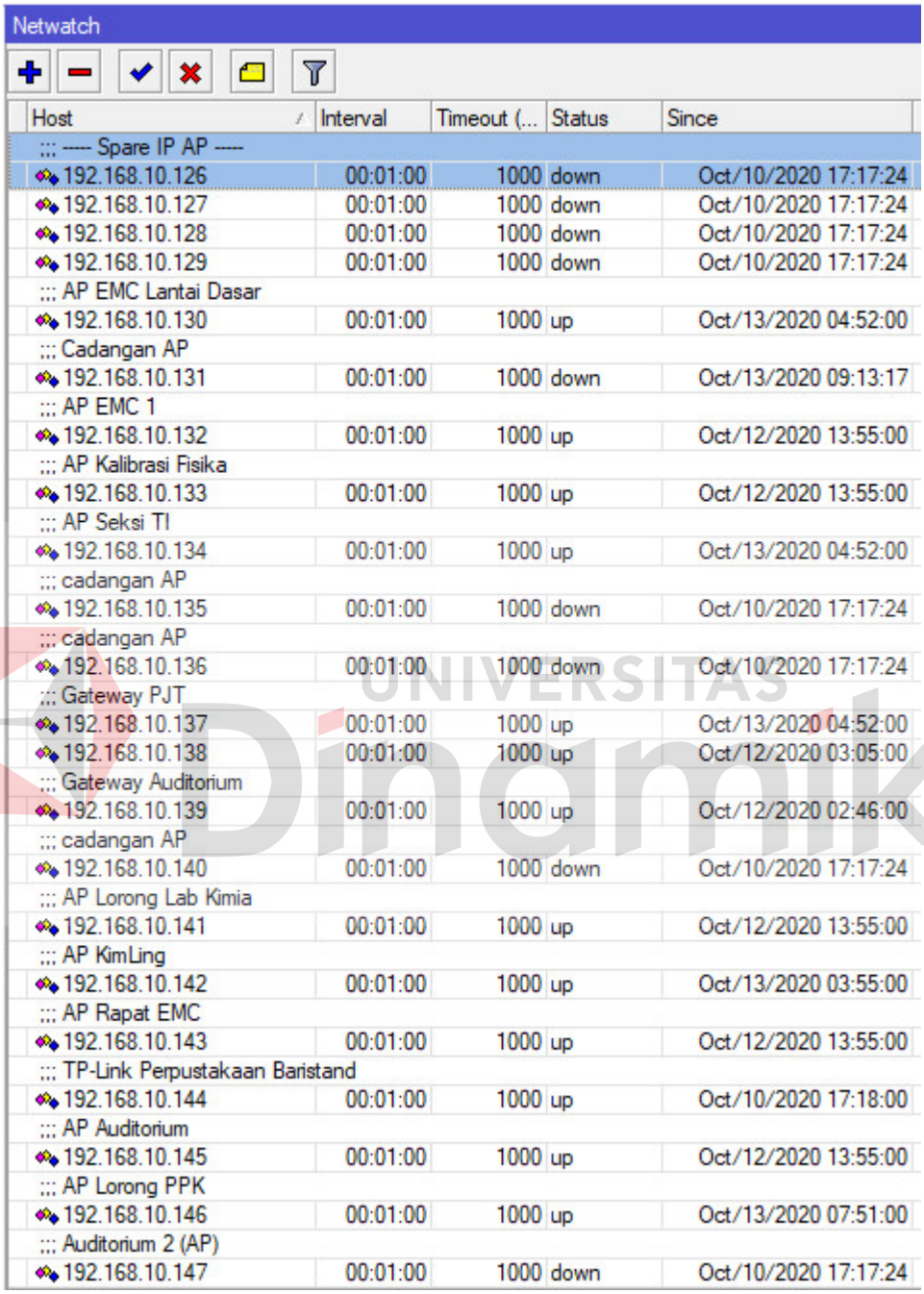


Gambar 37 Hasil akhir mangle bandwidth priority Google Meet

4.8 Membuat *Monitoring* Perangkat *Access Point*

Newatch merupakan salah satu fitur MikroTik yang berfungsi untuk memantau kondisi *host* dalam kasus ini adalah perangkat *access point*. Untuk

mempermudah pemantauan, MikroTik sudah menyediakan fitur ini. Untuk mengakses fitur ini bisa dari menu ***Tools > Netwatch***.



Host	Interval	Timeout (...	Status	Since
;;; ----- Spare IP AP -----				
192.168.10.126	00:01:00	1000	down	Oct/10/2020 17:17:24
192.168.10.127	00:01:00	1000	down	Oct/10/2020 17:17:24
192.168.10.128	00:01:00	1000	down	Oct/10/2020 17:17:24
192.168.10.129	00:01:00	1000	down	Oct/10/2020 17:17:24
;;; AP EMC Lantai Dasar				
192.168.10.130	00:01:00	1000	up	Oct/13/2020 04:52:00
;;; Cadangan AP				
192.168.10.131	00:01:00	1000	down	Oct/13/2020 09:13:17
;;; AP EMC 1				
192.168.10.132	00:01:00	1000	up	Oct/12/2020 13:55:00
;;; AP Kalibrasi Fisika				
192.168.10.133	00:01:00	1000	up	Oct/12/2020 13:55:00
;;; AP Seksi TI				
192.168.10.134	00:01:00	1000	up	Oct/13/2020 04:52:00
;;; cadangan AP				
192.168.10.135	00:01:00	1000	down	Oct/10/2020 17:17:24
;;; cadangan AP				
192.168.10.136	00:01:00	1000	down	Oct/10/2020 17:17:24
;;; Gateway PJT				
192.168.10.137	00:01:00	1000	up	Oct/13/2020 04:52:00
192.168.10.138	00:01:00	1000	up	Oct/12/2020 03:05:00
;;; Gateway Auditorium				
192.168.10.139	00:01:00	1000	up	Oct/12/2020 02:46:00
;;; cadangan AP				
192.168.10.140	00:01:00	1000	down	Oct/10/2020 17:17:24
;;; AP Lorong Lab Kimia				
192.168.10.141	00:01:00	1000	up	Oct/12/2020 13:55:00
;;; AP KimLing				
192.168.10.142	00:01:00	1000	up	Oct/13/2020 03:55:00
;;; AP Rapat EMC				
192.168.10.143	00:01:00	1000	up	Oct/12/2020 13:55:00
;;; TP-Link Perpustakaan Baristand				
192.168.10.144	00:01:00	1000	up	Oct/10/2020 17:18:00
;;; AP Auditorium				
192.168.10.145	00:01:00	1000	up	Oct/12/2020 13:55:00
;;; AP Lorong PPK				
192.168.10.146	00:01:00	1000	up	Oct/13/2020 07:51:00
;;; Auditorium 2 (AP)				
192.168.10.147	00:01:00	1000	down	Oct/10/2020 17:17:24

Gambar 38 Hasil pemantauan kondisi *access point*

1. *Host* : Informasi *IP address* perangkat yang akan dipantau.
2. *Interval* : *Netwatch* berkerja dengan mengirimkan *ping*. Pada parameter *interval*, bisa ditentukan jangka waktu *router* untuk mengirimkan *ping* untuk mengecek kondisi *host*.
3. *Time Out* : Jangka waktu berapa lama host akan dianggap down jika ping yang dikirim dari *router* tidak mendapat respon (unreachable).

Pada gambar 38, terlihat bahwa konfigurasi *netwatch* akan memantau *host* dengan blok *IP address* 192.168.10.x. Informasi status tertera "*up*" karena *router* bisa melakukan *ping* ke *IP address* tersebut. Jika *router* gagal mengirimkan *ping*, maka status akan berubah menjadi "*down*".

BAB V

PENUTUP

5.1 Kesimpulan

Dari hasil Kerja Praktik yang dilakukan di Balai Riset dan Standardisasi Industri Surabaya, dapat diambil beberapa kesimpulan pada hasil konfigurasi yang sudah diterapkan, dengan detail sebagai berikut:

1. Pengamanan *router* sudah dilakukan terbukti dengan tidak ditemukannya lagi serangan melalui port *telnet* maupun *ssh.*
2. Penambahan *mangle rule* untuk memisahkan antara *taffic browsing* dengan *traffic teleconference* sudah berjalan dengan baik, dibuktikan dengan testimoni dari beberapa pegawai yang melakukan *teleconference.*
3. Perubahan jumlah alokasi *IP* yang sebelumnya masih menggunakan *subnet* /24 menjadi *subnet* /23 menjadikan jumlah alokasi *IP* yang kosong menjadi sejumlah 254 *IP* yang sebelumnya hanya tersisa sekitar 100 *IP.*
4. Pembagian *bandwidth* sudah sesuai dengan tujuan dari admin jaringan kantor BARISTAND Industri Surabaya dengan alokasi *bandwidth* untuk setiap pengguna yang sudah dikalkulasi dengan matang.
5. Penambahan fitur pemantauan perangkat *access point* sudah berjalan normal dan sudah digunakan untuk melihat kondisi perangkat tanpa harus melihat langsung ke lokasi perangkat terpasang.

5.2 Saran

Beberapa saran yang bisa diberikan oleh penulis untuk pengembangan Kerja Praktik ini adalah:

1. Menurut pengamatan penilis, admin jaringan juga perlu untuk melakukan pencadangan konfigurasi *router* secara berkala, agar ketika terjadi masalah pada *router* tidak sampai menimbulkan *down time* yang lama.
2. Selain itu, melakukan *update* pada versi RouterOS juga menjadi poin penting karena dari pihak *developer* RouterOS pasti sudah melengkapi atau membenahi *bug* yang ada pada versi RouterOS sebelumnya, sehingga dari segi keamanan dan performa juga akan mengalami peningkatan.

DAFTAR PUSTAKA

Prakasa, J. E. W., 2018. *Konsep Dasar Jaringan Komputer.* Malang: UIN Maliki Press.

TEKNOLOGI, C. S., n.d. *www.mikrotik.co.id.* [Online] Available at: http://mikrotik.co.id/artikel_lihat.php?id=53 [Accessed 25 September 2020].

TEKNOLOGI, C. S., n.d. *www.mikrotik.co.id.* [Online] Available at: http://mikrotik.co.id/artikel_lihat.php?id=263 [Accessed 30 September 2020].