

IMPLEMENTASI MANAJEMEN BANDWIDTH UNTUK VIDEO CONFERENCE DENGAN METODE FIREWALL MANGLE PADA ROUTER *RB951-2n*

Abdul Rahman

Teknik Informatika, STMIK GI MDP, Palembang
Email Korespondensi : arahman@mdp.ac.id

ABSTRAK

Kegiatan belajar dari rumah atau bekerja dari rumah pada masa Pandemi Covid-19 telah meningkatkan trafik penggunaan akses internet. Fasilitas video conference merupakan kebutuhan yang realistis agar penyampaian pembelajaran, rapat atau laporan pekerjaan bisa berlangsung dengan baik. Oleh sebab itu sangat penting untuk menjaga kestabilan konektivitas jaringan internet terutama bandwidth untuk paket data video conference. Firewall mangle dan metode queue tree merupakan suatu solusi yang dapat diterapkan untuk melakukan manajemen bandwidth pada router Mikrotik RB951-2n. Firewall mangle membut mark connection dan mark packet untuk menandai trafik mana yang menggunakan aplikasi video conference, dimana dalam penelitian ini menggunakan aplikasi Zoom. Mark paket yang dibuat diterapkan pada model antrian queue tree untuk memberikan prioritas penggunaan bandwidth untuk vide conference. Hasil pengujian dari konfigurasi router RB951-2n dengan menggunakan ip firewall mangle dan queue tree menunjukkan bahwa penggunaan bandwidth untuk video conference menggunakan aplikasi Zoom(paket_zoom) lebih di prioritaskan dari pada akses data yang lain dalam gal ini paket_browsing.

Kata kunci: *Firewall, Mangle, queue, bandwidth, Mikrotik, video conference*

ABSTRACT

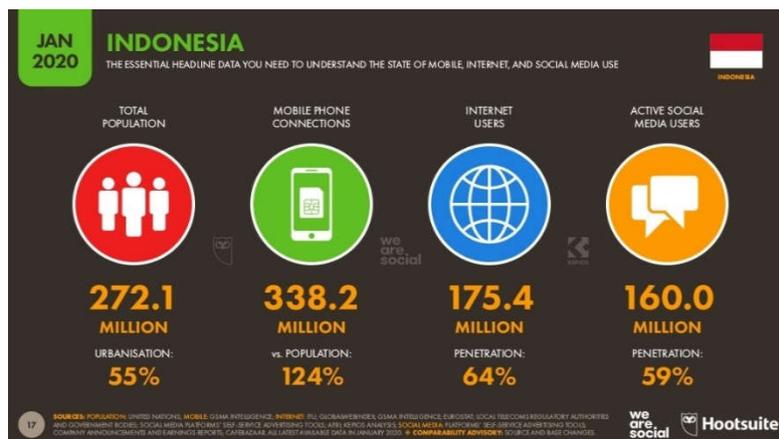
Learning from home or working from home during the Covid-19 Pandemic has increased traffic using internet access. Video conferencing facilities are a realistic need so that the delivery of learning, meetings or work reports can take place properly. Therefore it is very important to maintain the stability of internet network connectivity, especially bandwidth for video conferencing data packages. Firewall mangle and queue tree method is a solution that can be applied to perform bandwidth management on the Mikrotik RB951-2n router. The firewall mangle makes connection mark and packet mark to mark which traffic is using the video conference application, which in this study uses the Zoom application. The packet mark created is applied to the queue tree queue model to give priority to bandwidth usage for video conferencing. The test results of the RB951-2n router configuration using ip firewall mangle and queue tree show that the bandwidth usage for video conferencing using the Zoom application (packet_zoom) is prioritized over other data access in this package_browsing.

Keywords: *Firewall, Mangle, queue, bandwidth, Mikrotik, video conference*

PENDAHULUAN

Jaringan komputer terdiri dari kumpulan dari beberapa perangkat komputer dan peralatan pendukung lainnya yang terhubung dalam satu kesatuan dan saling terkoneksi[1]. Perkembangan pengguna di internet terus mengalami peningkatan secara signifikan, berdasarkan hasil *survey We Are Social* pada Januari 2020 pengguna internet di Indonesia sebanyak 172,4 juta, pengguna *social media* di Indonesia sebanyak 160 juta dan koneksi seluler di Indonesia mencapai 338,2 juta(jumlahnya 124% dari total penduduk Indonesia seperti yang terlihat pada Gambar 1[2].

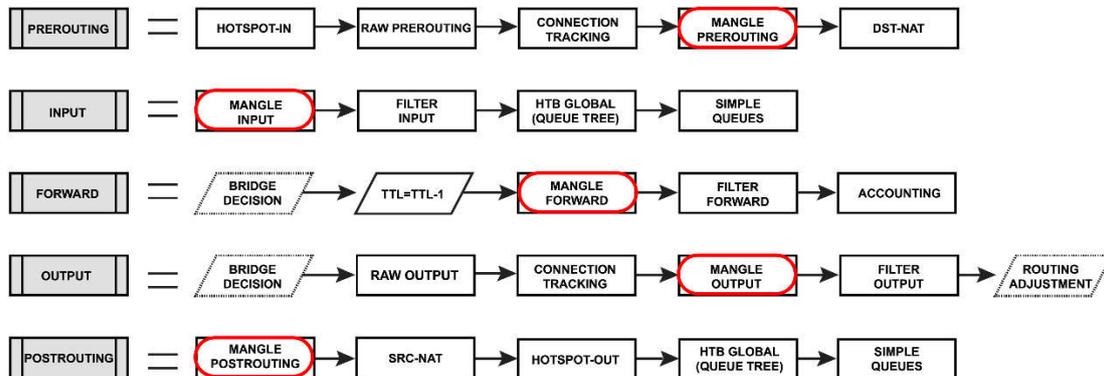
Pada masa pandemi Covid-19 yang telah berlangsung sejak awal tahun 2020 menyebabkan berbagai kegiatan banyak dilakukan dirumah secara daring atau yang lebih populer dengan sebutan *Work From Home (WFH)* atau bekerja dari rumah. Kegiatan belajar dan mengajar baik di sekolah maupun perguruan tinggi merupakan salah satu kegiatan yang menggunakan belajar secara daring dari rumah di masa pandemi Covid-19 ini. Kegiatan belajar mengajar dan bekerja yang digelar dalam jaringan (*online*) selama pandemi membuat lalu lintas data melesat tajam. Ketua Umum Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) Jamalul Izza mengatakan bahwa selama pembatasan sosial skala besar diterapkan terjadi kenaikan lalu lintas data sekitar 20 sampai 25 persen[3]. Kebutuhan akses ke jaringan internet saat ini diantaranya untuk *browsing*, sosial media, *streaming* dan *game*. Kebutuhan akses internet tersebut dapat ditandai dengan melakukan beberapa cara, misalnya untuk *browsing* dapat di tandai dari protokol *tcp port 80* dan *port 443*, untuk aplikasi sosial media seperti *facebook*, *instagram*, *twitter* dan *whatsapp* dapat menggunakan *marking* pada layer 7, aplikasi *game* dan *streaming* dapat ditandai dari *port* aplikasinya baik untuk protokol *tcp* dan *udp*. Proses belajar mengajar secara daring menggunakan *video conference* agar dapat berjalan dengan baik tanpa adanya gangguan dapat dilakukan dengan salah satu cara yaitu penggunaan *bandwith video conference* di prioritaskan pada kebutuhan akses data video streaming. Router melakukan banyak fungsi di jaringan komputer *modern*, meneruskan lalu lintas antara dua atau lebih jaringan lokal dalam satu organisasi atau perusahaan[4]. Salah satu yang bisa dilakukan router adalah mememanajemen penggunaan *bandwith* internet.



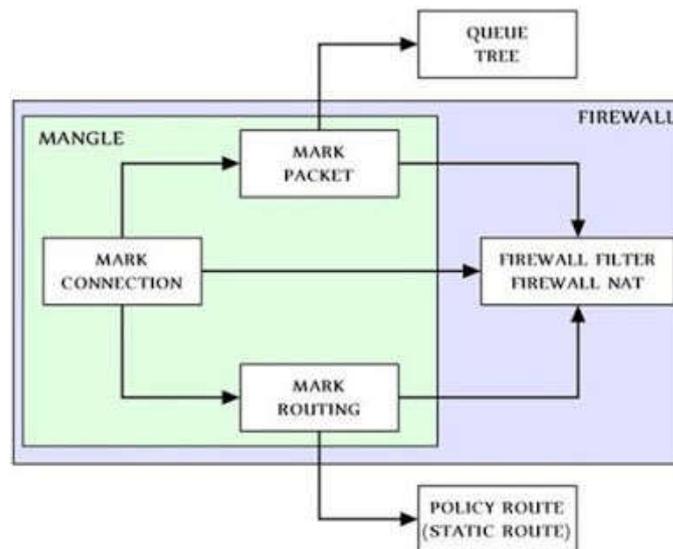
Gambar 1. Hasil Survey Jumlah Pengguna Internet di Indonesia[2]

Penelitian terhadap manajemen *bandwith* pada router Mikrotik telah dilakukan diantaranya Analisis performa RouterOs pada jaringan internet[5], dimana pada penelitian ini melakukan analisis performa koneksi jaringan internet pada RouterOs, penggunaan *mangle* untuk menandai koneksi yang masuk dan keluar router sedangkan untuk manajemen *bandwith* digunakan *queue tree*. Fatsyahrina melakukan penelitian untuk implementasi manajemen *bandwith* menggunakan *queue tree* untuk membatasi penggunaan *bandwith* dan *firewall mangle* untuk menandai trafik yang masuk dan keluar router, dimana routerOs yang digunakan adalah Mikrotik OS 2.9.27[6]. Pada penelitian ini yang dilakukan ini bertujuan untuk mememanajemen penggunaan *bandwith*, mengurangi terjadinya antrian pada jaringan dan memberikan prioritas paket data yang penting, dalam hal ini paket data untuk kelancaran proses belajar dan mengajar secara daring melalui *video conference*. Mikrotik RouterOS mempunyai 5 jenis *firewall*, yaitu: *Connection tracking*, *Filters*, *NAT*, *Mangle* dan *RAW*. *Firewall mangle* merupakan salah satu fitur *Firewall* yang ada pada router Mikrotik yang mempunyai fungsi untuk melakukan *marking*(penandaan) pada

suatu paket data tertentu, dimana paket data yang telah di tandai ini nantinya dapat digunakan oleh beberapa fitur yang ada pada router Mikrotik[7]. Aturan pada *Firewall mangle* mempunyai 5 *chain* yang telah ditentukan dan tidak dapat dihapus, yaitu: *Prerouting*, *Input*, *Output*, *Forward* dan *Postrouting* seperti yang terlihat pada Gambar 2. Ada 3 jenis *marking* yang dapat digunakan pada routerOS Mikrotik, yaitu: *Connection Mark*, *Packet Mark* dan *Route Mark* seperti yang ada pada Gambar 3.



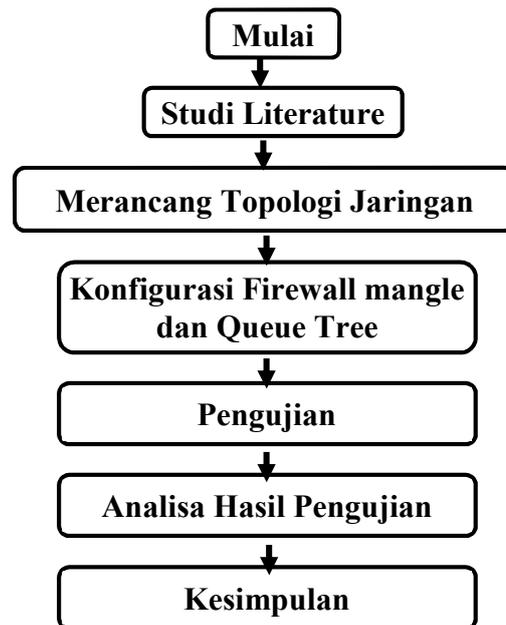
Gambar 2. Firewall Mangle Rules[7]



Gambar 3. Jenis Marking pada RouterOS Mikrotik

METODE PENELITIAN

Penelitian ini melakukan pengujian terhadap manajemen *bandwith* menggunakan *firewall mangle* dan *queue* terhadap paket data yang digunakan dengan router RB951-2nd sebagai *access point*. Data diperoleh dari pengamatan penggunaan *bandwith* oleh klien pada *queue tree* yang dibuat dengan *firewall mangle* pada masing-masing penggunaan paket data yang telah ditandai (*marking*) terhadap akses data dalam kelompok *streaming*(aplikasi *zoom*), *browsing*, *sosmed*, dan *youtube*. Pada tahap awal penelitian dilakukan studi literatur terkait konfigurasi *firewal mangle* dan *queue tree* pada router Mikrotik, kemudian pembangunan topologi jaringan *access point* untuk topologi *SOHO*(*Small Office Home Office*) menggunakan router board Mikrotik RB951-2n. Pada tahap selanjutnya dilakukan konfigurasi *firewall mangle* dan *queue tree* pada router Mikrotik RB951-2nd. Konfigurasi router yang telah dibuat selanjutnya dilakukan pengujian, pengamatan dan analisa dari data hasil pengujian. Tahapan metodologi penelitian yang dilakukan dapat dilihat pada Gambar 3.

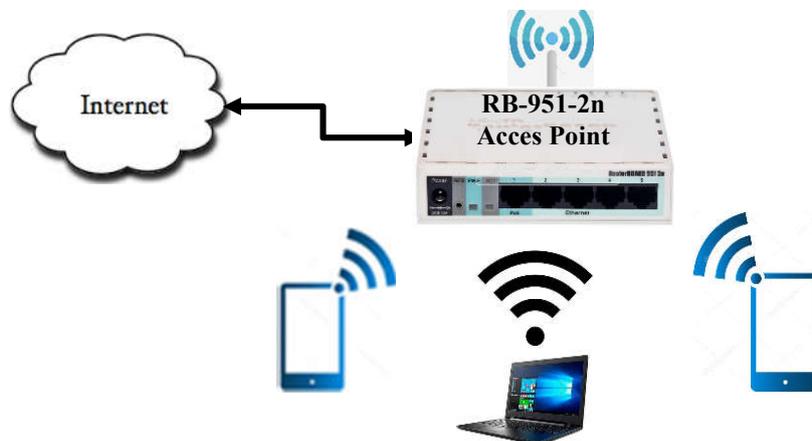


Gambar 4. Metodologi Penelitian

HASIL DAN PEMBAHASAN

Topologi Jaringan

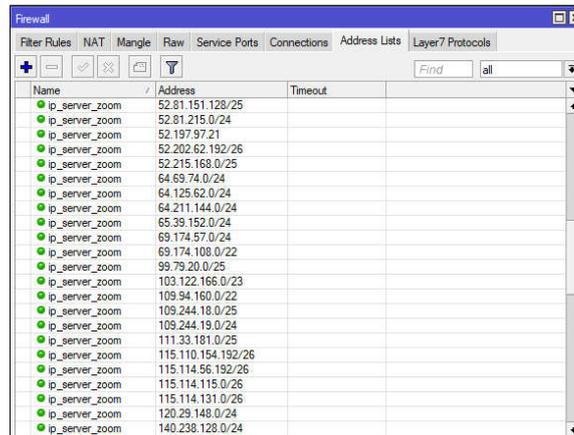
Topologi jaringan komputer yang digunakan dalam penelitian ini menggunakan Topologi *SOHO* dengan menggunakan router mikrotik RB951-2n sebagai *access point*, dimana semua *client* terkoneksi melalui jaringan *wireless* pada *interface wlan1* di RB951-2n pada frekuensi 2,4 GHz, seperti yang terlihat pada gambar 5.



Gambar 5. Topologi Jaringan

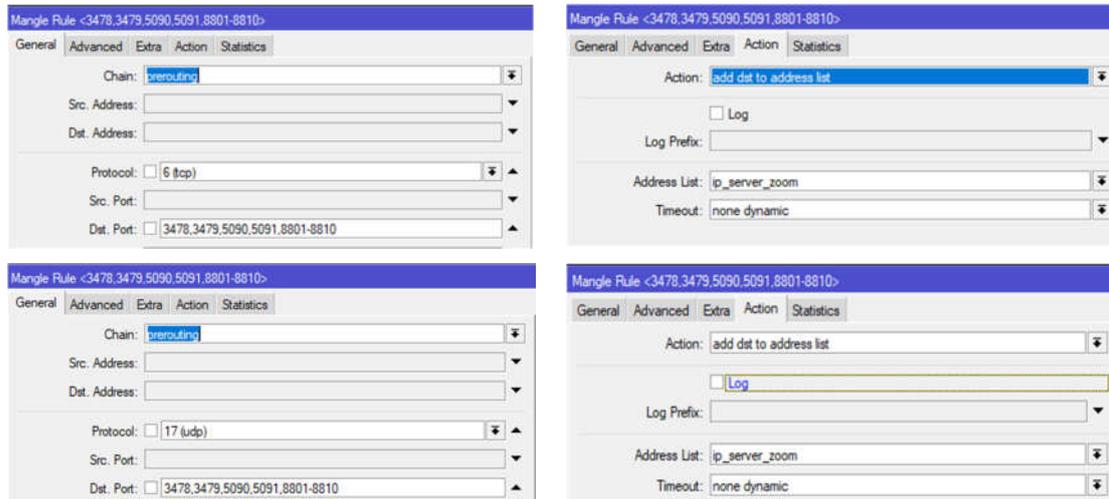
Konfigurasi *Firewall Mangle*

Konfigurasi *Firewall Mangle* dan *queue tree* yang dilakukan pada penelitian ini memprioritaskan penggunaan pelaksanaan belajar mengajar melalui *video conference* menggunakan aplikasi *Zoom*. Sebelum dilakukan konfigurasi pada *firewall mangle*, maka perlu dikonfigurasi untuk *address list* dari *IP server Zoom*. Aplikasi *zoom* sendiri telah memberikan daftar *IP server Zoom* yang disediakan[8]. *IP server Zoom* tersebut kita tambahkan pada *address list* di *router mikrotik* di menu *IP/Firewall/Address List*, hasilnya seperti pada gambar 6.



Gambar 6. Konfigurasi Address List untuk IP Server Zoom

Aplikasi Zoom menggunakan 2 protokol yaitu TCP dan UDP dengan daftar penggunaan port berikut: 3478, 3479, 5090, 5091, 8801-8810 termasuk juga port 80 dan 443[9]. Konfigurasi IP firewall mangle untuk memasukan destination port dari aplikasi Zoom tersebut dengan menggunakan konfigurasi pada router seperti pada gambar 7.



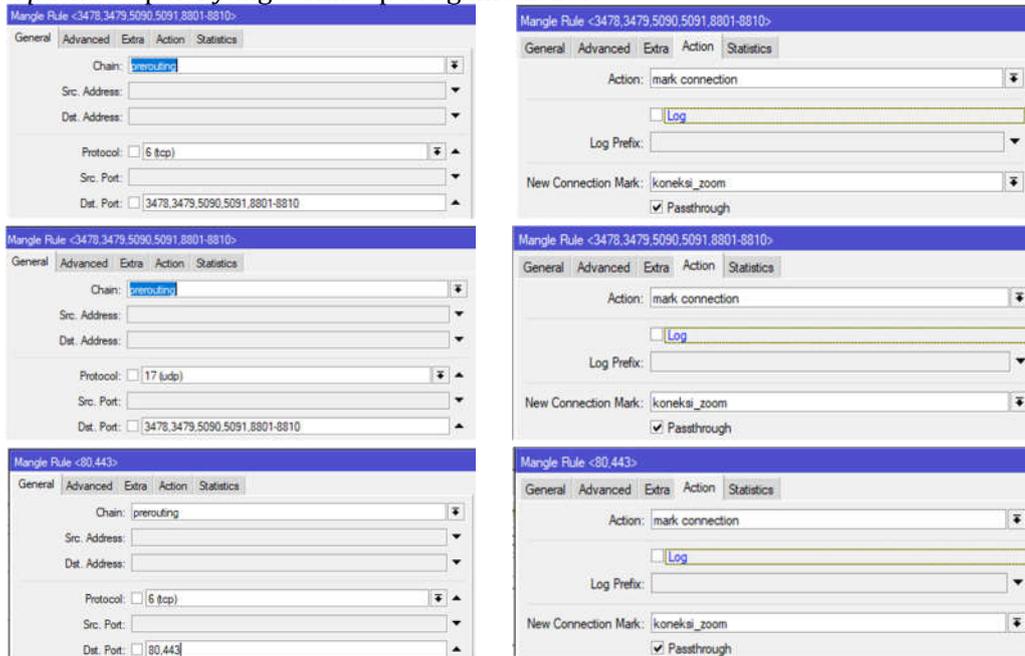
Gambar 7. Konfigurasi Firewall Mangle untuk server Zoom protokol TCP dan UDP

Pada konfigurasi gambar 7 router telah menambahkan secara otomatis ke dalam address list ip_server_zoom jika ada IP server Zoom yang baru belum terdaftar dalam address list ip_server_zoom. Selanjutnya pada mangle dibuat konfigurasi untuk menangkap jika ada trafik koneksi yang menggunakan aplikasi zoom baik melalui protokol tcp maupun udp dengan menambahkan rule baru pada firewall mangle dengan action mark-connection dan destination port 3478, 3479, 5090, 5091, 8801-8810 serta port 80 dan 443, seperti pada gambar 8.

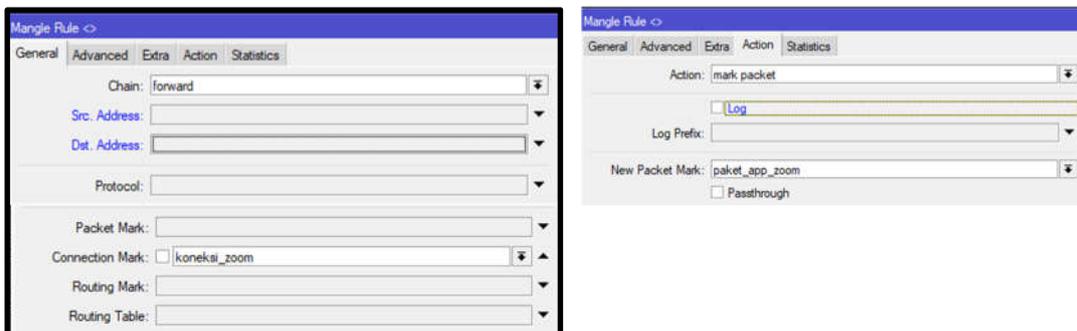
Pada rule untuk protokol tcp dengan destination-port 80 dan 443 ditambahkan dengan destination-address-list ke ip_server_zoom bertujuan untuk memastikan bahwa yang browsing selain menggunakan ip server zoom tidak tertangkap oleh rule ini. Setelah rule konfigurasi mangle untuk mark-connection dibuat, selanjutnya untuk implementasi ke manajemen bandwidth menggunakan queue tree dengan membuat sebuah rule mangle mark-packet seperti pada gambar 8.

Proses selanjutnya dibuat mark connection dan mark packet untuk paket yang digunakan buat browsing. Hal ini nanti dapat digunakan pada saat melakukan manajemen

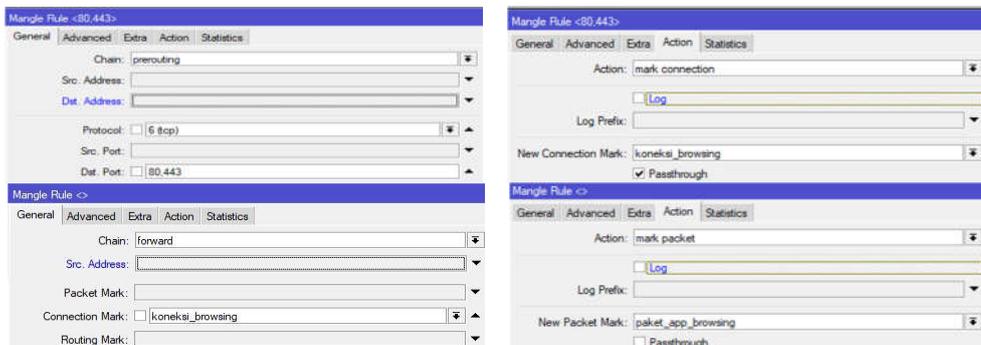
bandwith untuk dapat memisahkan mana koneksi yang menggunakan aplikasi *zoom* dan mana koneksi yang tidak digunakan untuk aplikasi *zoom*, prioritas penggunaan *bandwith* ada pada penggunaan aplikasi *zoom*. Konfigurasi yang ditambahkan pada *IP firewall mangle* untuk koneksi *browsing* seperti gambar 9, sehingga pada *IP Firewall mangle* sudah dibuat 8 buah *rule* yang terdiri dari 3 kategori, yaitu: *add dst to address list*, *mark connection* dan *mark packet* seperti yang terlihat pada gambar 10.



Gambar 8 Konfigurasi untuk *Mark-Connection* Aplikasi Zoom



Gambar 9. Konfigurasi *Firewall Mangle* untuk *Mark-packet*



Gambar 10. Konfigurasi *Firewall Mangle* untuk *mark packet* dan *mark Connection* paket *browsing*

#	Action	Chain	Src. Address	Dst. Address	Proto...	Packet Mark	Connection Mark	Bytes	Packets	Comme...
--add dst to address list										
0	add dst to address list	pre-routing		6 (tcp)				0 B	0	
1	add dst to address list	pre-routing		17 (u...				0 B	0	
--mark connection										
2	mark connection	pre-routing		6 (tcp)				0 B	0	
3	mark connection	pre-routing		17 (u...				372.1 MB	366 707	
4	mark connection	pre-routing		6 (tcp)				2113.6 KB	14 181	
--mark packet										
5	mark packet	forward					koneksi_zoom	763.5 MB	746 814	
--mark connection										
6	mark connection	pre-routing		6 (tcp)	no-mark			20.4 MB	256 766	
--mark packet										
7	mark packet	forward					Koneksi Browsing	481.8 MB	634 021	

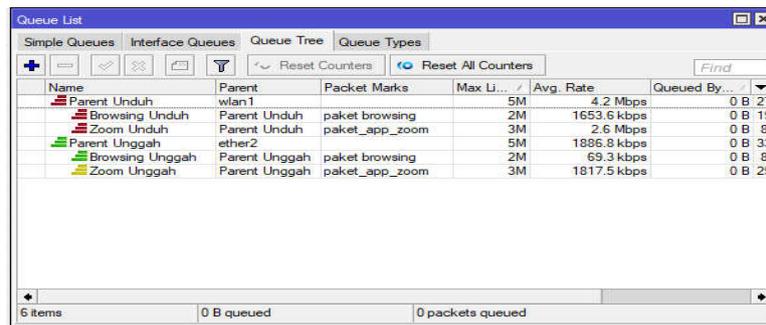
Gambar 11. Konfigurasi IP Firewall Mangle

Manajemen Bandwith

Konfigurasi pada *IP Firewall mangle* menghasilkan *mark connection* dan *mark packet*. *Mark packet* yang telah dibuat terdiri dari 2, yaitu: *mark packet koneksi_zoom* dan *mark packet koneksi_browsing*. Manajemen *bandwith* untuk membuat prioritas penggunaan *bandwith* pada aplikasi *zoom* digunakan *queue tree*. *Mark-packet* yang telah dibuat akan digunakan untuk melakukan limitasi *bandwith* pada *queue tree*. Untuk *parent queue* dibagi menjadi 2 buah *parent*, yaitu *parent unduh* dan *parent unggah*. *Parent unggah* adalah paket dari klien *router* menuju ke *internet*, sedangkan *parent unduh* merupakan paket dari *internet* yang menuju ke klien *router*. Konfigurasi yang dibuat pada *parent unggah*, untuk *parentnya* menggunakan *interface ether2* karena *interface* ini yang terhubung ke *internet* dengan tipe *queue* yang digunakan adalah *pcq upload* dan dibatas untuk maksimum *bandwithnya* adalah 5 Mbps, sedangkan pada *parent unduh*, untuk *parentnya* menggunakan *interface wlan1* karena *interface* ini yang terkoneksi ke klien dengan tipe *queue* yang digunakan adalah *pcq download* dan besarnya *bandwith* dibatasi pada maksimum 5 Mbps. Pada *parent unggah* dibuat 2 buah *parent child* yaitu untuk paket *zoom* dan paket *browsing*, dimana paket *zoom* diberikan maksimum *bandwithnya* 3 Mbps dan paket *browsing* diberikan 2 Mbps. Sedangkan untuk *parent unduh* juga dibuat 2 buah *parent child* untuk paket *zoom* dan paket *browsing* dengan maksimum *bandwith* untuk paket *zoom* adalah 3 Mbps dan paket *browsing* sebesar 2 Mbps seperti gambar 12.

Queue Name	Parent	Packet Marks	Queue Type	Priority	Bucket Size	Limit At	Max Limit	Burst Limit	Burst Threshold	Burst Time
Browsing Unduh	Parent Unduh	paket browsing	pcq-download-default	8	0.100		2M			
Zoom Unduh	Parent Unduh	paket_app_zoom	pcq-download-default	8	0.100		3M			
Browsing Unggah	Parent Unggah	paket browsing	pcq-upload-default	8	0.100		2M			
Zoom Unggah	Parent Unggah	paket_app_zoom	pcq-upload-default	8	0.100		3M			

Gambar 12. Konfigurasi queue tree



Name	Parent	Packet Marks	Max Li...	Avg. Rate	Queued By...
Parent Unduh	wlan1		5M	4.2 Mbps	0 B 27
Browsing Unduh	Parent Unduh	paket browsing	2M	1653.6 kbps	0 B 19
Zoom Unduh	Parent Unduh	paket_app_zoom	3M	2.6 Mbps	0 B 8
Parent Unggah	ether2		5M	1886.8 kbps	0 B 33
Browsing Unggah	Parent Unggah	paket browsing	2M	69.3 kbps	0 B 8
Zoom Unggah	Parent Unggah	paket_app_zoom	3M	1817.5 kbps	0 B 25

Gambar 13. Hasil Pengamatan pada Queue Tree

Hasil Pengujian

Setelah dilakukan pengujian dengan membuka aplikasi *zoom* pada 2 buah klien dan melakukan *browsing* yang dilakukan oleh 5 klien yang terhubung ke *access point* sesuai topologi yang dibuat, maka didapatkan bahwa aplikasi *zoom* dapat berjalan lancar walaupun dibatasi hanya 3 Mbps untuk 2 aplikasi *zoom* yang dibuka walaupun pada saat yang bersamaan diberikan gangguan trafik dengan adanya 5 klien yang melakukan *browsing* dan juga membuka *youtube*. Pemantauan manajemen *bandwith* menggunakan *queue tree* dapat dilihat pada gambar 12.

Berdasarkan hasil ini, maka implementasi manajemen *bandwith* menggunakan *queue tree* dengan terlebih dahulu melakukan konfigurasi *ip firewall mangle* untuk menandai paket yang akan dilakukan manajemen *bandwith*nya dapat digunakan untuk menjaga agar koneksi *video conference* menggunakan aplikasi *zoom* tidak terganggu dengan banyaknya trafik penggunaan *bandwith* pada jaringan *internet* yang digunakan. Pada pengujian tersebut jika untuk paket *zoom* dibatasi 3 Mbps dengan tujuan untuk melihat bahwa prioritas *bandwith* yang digunakan pada jalur *internet* diutamakan untuk paket *zoom*, sehingga untuk implementasinya paket *zoom* pada konfigurasi *queue tree* pada *bandwith download* dan *upload* dibuat *unlimited* artinya jika *bandwith internet* adalah 10 Mbps maka prioritas untuk paket *zoom* bisa mencapai 10 Mbps sedangkan untuk pengguna yang melakukan *browsing* hanya dapat alokasi 2 Mbps.

KESIMPULAN

Penerapan *mark connection* dan *mark packet* untuk *video conference* pada aplikasi *zoom* melalui pengaturan *firewall mangle* di *routerboard* mikrotik RB951-2n dapat digunakan untuk melakukan manajemen *bandwith* dengan memberikan prioritas penggunaan *bandwith* kepada paket data *video conference* melalui aplikasi *zoom* melalui metode *queue tree*. Pada penelitian ini pembagian *bandwith* pada jaringan dibagi ke dalam 2 kelompok, yaitu *video conference* menggunakan aplikasi *zoom* dan untuk *browsing* (protokol *tcp*, port 80 dan 443), dimana prioritas penggunaan *bandwith* diperuntukkan aplikasi *Zoom*. Hasil dari pengujian menunjukkan bahwa penggunaan *bandwith* untuk aplikasi *Zoom* lebih diprioritas.

REFERENSI

- [1] Madcoms, *Sistem Jaringan Komputer untuk Pemula*. Yogyakarta: Andi Publisher, 2010.
- [2] we are social, "Digital 2020 Indonesia," 2020. [Online]. Available: <https://datareportal.com/reports/digital-2020-indonesia>. [Accessed: 28-Sep-2020].
- [3] L. D. Jatmiko, "Pandemi Covid-19 Dorong Kenaikan Trafik Data hingga 25 Persen," *Bisnis.com*, 2020. [Online]. Available: <https://teknologi.bisnis.com/read/20200813/101/1278818/pandemi-covid-19-dorong-kenaikan-trafik-data-hingga-25-persen>. [Accessed: 28-Sep-2020].

- [4] S. Alabady, "Design and Implementation of a Network Security Model for Cooperative Network," *Int. Arab J. e-Technology*, vol. 1, no. 2, pp. 26–36, 2009.
- [5] T. Rahman, S. Sumarna, and H. Nurdin, "Analisis Performa RouterOS MikroTik pada Jaringan Internet," *Ingénierie Des Systèmes D'information*, vol. 5, no. 1, pp. 178–192, 2020.
- [6] F. Fitriastuti and D. P. Utomo, "Implementasi Bandwith Management dan Firewall System Menggunakan," *J. Tek.*, vol. 4, no. October, pp. 46–54, 2017.
- [7] MikroTik, "Firewall Basic Concepts," *MikroTik*. [Online]. Available: <https://help.mikrotik.com/docs/display/ROS/Basic+Concepts#space-menu-link-content>. [Accessed: 28-Sep-2020].
- [8] ZOOM, "Network firewall or proxy server settings for Zoom," *ZOOM*. [Online]. Available: <https://support.zoom.us/hc/en-us/articles/201362683-Network-firewall-or-proxy-server-settings-for-Zoom>. [Accessed: 30-Sep-2020].
- [9] ZOOM, "Network Firewall Settings for Meeting Connector," *ZOOM*. [Online]. Available: <https://support.zoom.us/hc/en-us/articles/202342006-Network-Firewall-Settings-for-Meeting-Connector>. [Accessed: 30-Sep-2020].

