JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER
VOL. 4. NO. 1 AGUSTUS 2018
E-ISSN: 2527-4864

IMPLEMENTASI INTERFACE VIRTUAL LOCAL AREA NETWORK DAN FIREWALL PADA MIKROTIK DAN SWITCH MANAJEMEN

Taufik Rahman

Manajemen Informatika
AMIK BSI Jakarta
http://www.bsi.ac.id
taufik.tkr@bsi.ac.id

Abstract—*Today the campus network is very important and plays an important role for every organization in it. To efficiently manage ethernet network, detailed and accurate knowledge of topology is required, such as network partitioning, performance prediction based on network topology as well as computer network security threats and network architecture is always a serious and important issue. Development of local area network (LAN) with the implementation of Virtual Local Area Network (VLAN) and firewall on MikroTik router and management switch will be tested as a solution for college application and management network. The vlan interface with vlan id as a differentiator on the MikroTik router on the bonding interface, combining the two ethernet into one using the rr balance mode, it can separate the network traffic so that broadcasts from the network can be minimized and become easy to monitor network usage trafc, detecting connection failures can traced based on PVID through switch management monitoring. The policy on network usage is done through a firewall on the campus MikroTik router so that it can monitor traffic and incoming and outgoing data packets. This is evidenced by some websites that should not be accessed, as well as with ports and network protocols.*
Keywords*: Network, Vlan, Firewall, MikroTik, Switch.*

Intisari— Saat ini jaringan kampus sangat penting dan memainkan peran penting untuk setiap organisasi didalamnya. Untuk mengelola jaringan ethernet secara efisien, pengetahuan rinci dan akurat dari topologi diperlukan, seperti partisi jaringan, prediksi kinerja didasarkan pada topologi jaringan begitu pula ancaman keamanan jaringan komputer dan arsitektur jaringan selalu merupakan masalah serius dan penting. Pengembangan jaringan lokal area (LAN) dengan implementasi Virtual Local Area Network (VLAN) dan *firewall* pada router MikroTik dan switch manajemen akan dicoba sebagai solusi untuk aplikasi dan manajemen jaringan perguruan tinggi. Interface *vlan* dengan *vlan* id sebagai pembedanya pada router MikroTik pada *interface* bonding, digabungkan nya dua ethernet menjadi satu menggunakan mode balance rr, maka dapat memisahkan trafik jaringan sehingga broadcast dari pada jaringan dapat diminimalisir dan menjadi mudah dalam memantau trafik penggunaan jaringan, mendeteksi kegagalan koneksi dapat ditelusuri berdasarkan PVID melalui monitoring switch manajemen. Kebijakan mengenai penggunaan jaringan dilakukan melalui *firewall* pada router MikroTik kampus sehingga dapat di monitoring trafik dan paket data yang masuk dan keluar. Hal ini di buktikan dengan beberapa website yang tidak boleh diakses, begitupun dengan port dan protokol jaringan.
Kata Kunci*: Jaringan, Vlan, Firewall, MikroTik, Switch.*

PENDAHULUAN

Jaringan lokal area berada di organisasi seperti perusahaan, universitas dan sebagainya. Dalam beberapa tahun terakhir, dengan perkembangan teknologi, jaringan ini menjadi skala besar dan terdiri dari sejumlah besar perangkat, dan membuat manajemen jaringan ini sulit dalam hal fleksibilitas karena kondisi kendala yang ditempati oleh perangkat dan kurangnya profesional manajemen yang terampil untuk jaringan ini(Kodama, Nakagawa, Tanouchi, & Kameyama, 2016). Saat ini jaringan kampus sangat penting dan memainkan peran penting untuk setiap organisasi didalamnya. Jaringan kampus adalah jaringan otonom yang berada di dalam tempat geografis lokal dan kadang-kadang mungkin jaringan area metropolitan, jumlah laptop di perguruan tinggi dan universitas telah meningkat tanpa henti, sehingga setiap laptop memiliki akses yang sama atau berbeda, seperti laptop mahasiswa yang mengakses ke jaringan internal lokal untuk perkuliahan, terdapat juga jaringan hanya bisa mengakses internet dan sebagainya. Paket broadcast dan multicast mencapai setiap segmen layer-2 dari LAN, apakah komputer tersebut dimaksudkan untuk menerima

paket tersebut atau tidak, demikian dapat menghabiskan bandwidth. Untuk mengelola jaringan ethernet secara efisien, pengetahuan rinci dan akurat dari topologi diperlukan, seperti partisi jaringan, prediksi kinerja didasarkan pada topologi jaringan begitu pula ancaman keamanan jaringan komputer dan arsitektur jaringan selalu merupakan masalah serius dan penting(Zhou & Ma, 2016).

Penelitian ini menggunakan beberapa referensi yang terkait dengan objek riset utama, antara lain oleh lehocine yang melakukan studi filter *vlan* dan mensegmentasi nya pada jaringan regular dan jaringan SDN(Lehocine & Batouche, 2017)

Sebuah algoritma untuk menemukan struktur topologi tata letak fisik jaringan Ethernet dengan informasi alamat penyuratan alamat yang tidak lengkap. Algoritma ini dapat menangani kedua switch layer-2 dengan switch VLAN dan layer-3. Menerapkan nya pada jaringan beberapa universitas, dan bekerja dengan baik di jaringan ini dibagi dengan VLAN. Dan ada banyak jaringan universitas dan kampus yang menggunakan VLAN berdasarkan divisi (Zhou & Ma, 2016)

Sistem yang memisahkan jaringan ke dalam beberapa kelompok jaringan virtual sebagai unit untuk komunikasi pada sistem yang disesuaikan dan mengatur komunikasi di antara kelompok-kelompok ini dengan mengaitkan klien sebagai perangkat pada sistem fisik dengan kelompok-kelompok tersebut. Sistem berfungsi sebagai perangkat lunak yang mendefinisikan fungsi dengan menggunakan paket tertanam yang dibuat oleh Virtual Network Interface Card (VNIC) dan informasi spesifik perangkat(Kodama et al., 2016)

Virtual Local Area Networks (VLAN) menyediakan pengelompokan logis dalam LAN yang digunakan untuk berbagai tujuan termasuk untuk membatasi trafik siaran dan untuk menyediakan lokalisasi trafik yang lebih baik(Hameed & Mian, 2015)

Untuk meningkatkan kinerja jaringan data center, meningkatkan bandwidth, mengurangi lalu lintas server dan penyimpanan, mengurangi investasi pemasangan kabel dan waktu penyebaran dengan mengisolasi jaringan pemantauan dan pengendalian sistem ke WLAN dan VLAN(Wiboonrat, 2014)

Ketika *firewall* dan VLAN digunakan bersama-sama di jaringan kampus, lalu lintas awal http berkurang lebih dari 7.5Bps dan setelah konvergensi lalu lintas menjadi kurang dari 2.0Bps(Ali, Rahman, & Hossain, 2013)

Merancang dan menerapkan kebijakan keamanan berdasarkan persyaratan dan tuntutan yang disajikan dengan skenario menggunakan peralatan MikroTik(Pauzhi & Coronel, 2015)

Tujuan dari penelitian ini bagaimana merencanakan dengan baik struktur jaringan, memastikan keamanan jaringan dan dengan demikian menjamin kelancaran kinerja jaringan, yang mana telah menjadi masalah yang sangat sulit dihadapi oleh pengelola jaringan kampus. Pengembangan jaringan lokal area (LAN) dengan implementasi Virtual Local Area Network (VLAN) dan *firewall* pada router MikroTik dan switch manajemen akan dicoba sebagai solusi untuk aplikasi dan manajemen jaringan perguruan tinggi.

BAHAN DAN METODE

Pada penelitian ini menggunakan perangkat keras MikroTik RB1100AHX2 sebagai router nya, D-Link DES 1210-52 sebagai switch manageable, dan AP-unifi series Pro sebagai access point. Selain itu menggunakan perangkat lunak RouterOS all_packages-ppc-6.33 yang diinstall pada router sehingga konfig *vlan* dan *firewall* dapat dilakukan.

Dalam penelitian menggunakan Network Development Life Cycle (NDLC) adalah metode yang digunakan pada pembuatan atau mendesain infrastruktur jaringan yang dapat memonitoring untuk mengetahui statistik dan performance jaringan(Rianafirin & Kurniawan, 2017), yang digunakan lima tahapan: analisa, desain, implementasi, monitoring dan manajemen.

Mendalami permasalahan terkait dengan jaringan lokal area, jaringan virtual lokal area dan keamanan, dengan melakukan studi pustaka yaitu dengan mengumpulkan data teoritis yang berasal dari jurnal, mempelajari buku-buku atau literature dengan maksud untuk mendapatkan teori dan bahan yang berkaitan dengan masalah *vlan* dan *firewall*.

Analisa Kebutuhan

Analisa Kebutuhan adalah analisa topologi jaringan yang sudah ada pada saat ini dan perencanaan implementasi topologi jaringan virtual lokal area yang akan dibuat beserta *firewall* nya sebagai keamanan jaringan, dimana *vlan* di buat dari gabungan beberapa *interface* Ethernet menjadi sebuah *interface* virtual yang disebut Bonding pada MikroTik, kemudian pada switch manajemen dibuat *vlan* yang jumlahnya sesuai dengan yang ada pada MikroTik.

Desain

Dari data yang sudah dianalisa pada tahap sebelumnya, pada tahap ini memberikan usulan yang dimaksudkan untuk lebih meningkatkan performansi, efisien dan efektifitas dari jaringan.

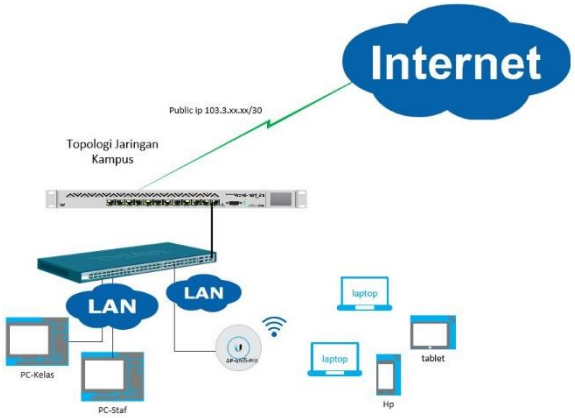
Adapun usulan yang diberikan berupa desain mengenai perangkat, topologi, skema, metode dan konsep yang akan digunakan.

Implementasi

Pada bagian ini, penggabungan topologi fisik yang sudah ada dengan topologi yang baru, yang sudah diuji. Dari pembuatan *interface* virtual, setting IP, konfigurasi routing, nat untuk masquerade sub-network nya, konfigurasi *firewall* rule, konfigurasi link aggregation pada switch, penambahan *vlan* pada switch manajemen dengan id yang sesuai pada router, menempelkan *vlan* pada Ethernet switch manajemen dilakukan pada tahap ini.

Manajemen

Pada tahapan ini, terkait dengan kebijakan user atau previlige yang dibuatkan dan ditentukan oleh pihak institusi, sehingga dapat berjalan dengan baik dan sesuai aturan.



Sumber: (Rahman, 2018)

Gambar 1. Topologi Jaringan Kampus

HASIL DAN PEMBAHASAN

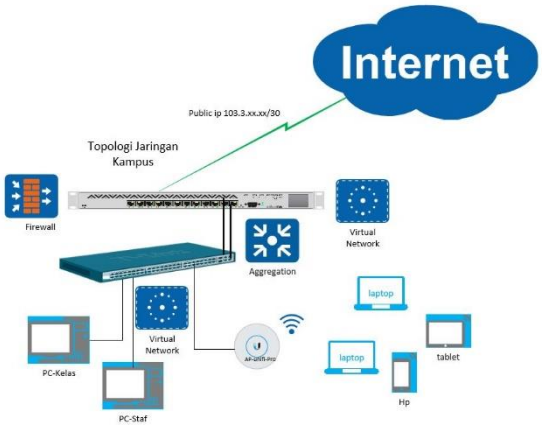
Dalam penelitian ini mengambil studi kasus jaringan lokal area pada salah satu instansi yang dijadikan sebagai objek nya, dimana terdapat koneksi internet yang melewati router MikroTik yang didalam nya terdapat beberapa network, kemudian dari router dihubungkan ke switch Dlink DES 1210-52 terdiri dari 48 ethernet 100mbps, 2 ethernet 1Gbps dan 2 port SFP. Dari switch dihubungkan dengan kabel UTP ke komputer, laptop melalui perangkat wireless atau AP(access point)Unifi hingga smartphone baik karyawan maupun mahasiswa. Selanjutnya koneksi jaringan digunakan untuk operasional kerja diantaranya sharing(file, printer), mengakases website intranet maupun internet, sebagaimana pada gambar 1. Adapun pembahasannya sebagai berikut.

A. Analisa Permasalahan

Dengan topologi jaringan pada gambar 1 terjadi broadcast storm yang diakibatkan dengan bertambah nya pengguna jaringan karena adanya kebijakan dari lembaga bahwa mahasiswa diwajibkan untuk membawa laptop untuk perkuliahan, absensi masuk dan akses ke materi ketika di ruang kelas dengan mengakses web intranet melalui AP Unifi yang terdapat pada setiap ruang kelas, begitu juga untuk ujian tengah dan akhir semester. Dari sisi keamanan jaringan juga perlu perhatian, diantaranya pembatasan jaringan karena privasi. Dari hal itu, maka solusi yang baik adalah dengan mengimplementasikan virtual local area network dan *firewall* dimulai dari router hingga switch.

B. Desain

Pada bagian desain dimulai membuat topologi jaringan pada gambar 2, pembuatan ip address, menentukan jumlah *interface vlan*, network address translation, routing pada MikroTik Router dan menentukan port Ethernet pada switch manajemen. Instalasi packet user-manager dan menentukan kebijakan terkait dengan *firewall* pada *interface vlan*.



Sumber: (Rahman, 2018)

Gambar 2. Jaringan Komputer Kampus dengan *interface vlan* dan *firewall* pada mikrotik dan switch manajemen

Koneksi jaringan kampus menggunakan internet 30 mbps untuk mendukung kegiatan proses belajar mengajar. Interface *vlan* di buat pada *router* MikroTik RB1100, dua Ethernet digabungkan menjadi satu *interface* bonding.
Interface bonding pada MikroTik dapat dilihat dengan CLI (Command Line Interface) menggunakan Putty dengan SSH pada ip router nya sebagai berikut

```
[taufik@MT_Kampus] > interface bonding pr detail
Flags: X - disabled, R - running
 0  R  name="bonding1"  mtu=1500  mac-address=D4:CA:6D:2A:A8:F9  arp=enabled slaves=ether4,ether5 mode=balance-rr primary=none link-monitoring=mii  arp-interval=100ms  arp-ip-targets=""
    mii-interval=100ms down-delay=0ms up-delay=0ms lacp-rate=1sec  transmit-hash-policy=layer-2-and-3 min-links=0
```

Pada *interface* bonding inilah dibuat *interface vlan* dan *vlan*-id sesuai dengan kebutuhan peruntukan nya, misal kelas, divisi. Berikut adalah detail dari *interface vlan* dan *vlan*-id nya.

```
[[taufik@MT_Kampus] > interface vlan pr detail
Flags: X - disabled, R - running, S - slave
 0  R  name="vlan1"  mtu=1500  mac-address=D4:CA:6D:2A:A8:F9  arp=enabled  vlan-id=1 interface=bonding1 use-service-tag=no
 1  R  name="vlan10"  mtu=1500  mac-address=D4:CA:6D:2A:A8:F9  arp=enabled  vlan-id=10 interface=bonding1 use-service-tag=no
 2  R  name="vlan20"  mtu=1500  mac-address=D4:CA:6D:2A:A8:F9  arp=enabled  vlan-id=20 interface=bonding1 use-service-tag=no
 3  R  name="vlan30"  mtu=1500  mac-address=D4:CA:6D:2A:A8:F9  arp=enabled  vlan-id=30 interface=bonding1 use-service-tag=no
 4  R  name="vlan40"  mtu=1500  mac-address=D4:CA:6D:2A:A8:F9  arp=enabled  vlan-id=40 interface=bonding1 use-service-tag=no
 5  R  name="vlan50"  mtu=1500  mac-address=D4:CA:6D:2A:A8:F9  arp=enabled  vlan-id=50 interface=bonding1 use-service-tag=no
 6  R  name="vlan60"  mtu=1500  mac-address=D4:CA:6D:2A:A8:F9  arp=enabled  vlan-id=60 interface=bonding1 use-service-tag=no
 7  R  name="vlan70"  mtu=1500  mac-address=D4:CA:6D:2A:A8:F9  arp=enabled  vlan-id=70 interface=bonding1 use-service-tag=no
 8  R  name="vlan80"  mtu=1500  mac-address=D4:CA:6D:2A:A8:F9  arp=enabled  vlan-id=80 interface=bonding1 use-service-tag=no
 9  R  name="vlan90"  mtu=1500  mac-address=D4:CA:6D:2A:A8:F9  arp=enabled  vlan-id=90 interface=bonding1 use-service-tag=no
10  R  name="vlan100"  mtu=1500  mac-address=D4:CA:6D:2A:A8:F9  arp=enabled  vlan-id=100 interface=bonding1 use-service-tag=no
11  R  name="vlan200"  mtu=1500  mac-address=D4:CA:6D:2A:A8:F9  arp=enabled  vlan-id=200 interface=bonding1 use-service-tag=no
12  R  name="vlan500"  mtu=1500  mac-address=D4:CA:6D:2A:A8:F9  arp=enabled  vlan-id=500 interface=bonding1 use-service-tag=no
13  R  name="vlan600"  mtu=1500  mac-address=D4:CA:6D:2A:A8:F9  arp=enabled  vlan-id=600 interface=bonding1 use-service-tag=no
```

Jika pada ip address terdapat x artinya ujung ip address tersebut disembunyikan untuk keamanan. IP address pada MikroTik kampus adalah sebagai berikut,

```
[taufik@MT_Kampus] > ip address pr detail
Flags: X - disabled, I - invalid, D - dynamic
 0   address=10.10.0.1/26 network=10.10.0.0 interface=vlan1 actual-interface=vlan1
 1   address=10.10.1.1/25 network=10.10.1.0 interface=vlan10 actual-interface=vlan10
 2   address=10.10.2.1/25 network=10.10.2.0 interface=vlan20 actual-interface=vlan20
 3   address=10.10.3.1/25 network=10.10.3.0 interface=vlan30 actual-interface=vlan30
 4   address=10.10.4.1/25 network=10.10.4.0 interface=vlan40 actual-interface=vlan40
 5   address=10.10.5.1/25 network=10.10.5.0 interface=vlan50 actual-interface=vlan50
 6   address=10.10.6.1/25 network=10.10.6.0 interface=vlan60 actual-interface=vlan60
 7   address=10.10.7.1/25 network=10.10.7.0 interface=vlan70 actual-interface=vlan70
 8   address=10.10.8.1/25 network=10.10.8.0 interface=vlan80 actual-interface=vlan80
 9   address=10.10.9.1/25 network=10.10.9.0 interface=vlan90 actual-interface=vlan90
10   address=10.10.10.1/25 network=10.10.10.0 interface=vlan100 actual-interface=vlan100
11   address=172.16.15.254/24 network=172.16.15.0 interface=vlan200 actual-interface=vlan200
12   address=103.3.67.xx/29 network=103.3.67.64 interface=ether1-icon actual-interface=ether1-Wan
13   address=10.15.15.1/27 network=10.15.15.0 interface=vlan500 actual-interface=vlan500
14   address=192.168.15.1/26 network=192.168.15.0 interface=vlan600 actual-interface=vlan600
```

Routing dibutuhkan supaya *interface* yang dibawah router dapat saling berkomunikasi. Berikut route pada MikroTik Kampus.

```
[[taufik@MT_Kampus] > ip route pr detail
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme, B - blackhole, U - unreachable, P - prohibit
 0 A S  ;;; gtw icon
     dst-address=0.0.0.0/0 gateway=103.3.67.65 gateway-status=103.3.67.65 reachable via ether1-Wan check-gateway=ping distance=1 scope=30 target-scope=10
 1   ADC  dst-address=10.10.0.0/26 pref-src=10.10.0.1 gateway=vlan1 gateway-status=vlan1 reachable distance=0 scope=10
 2   ADC  dst-address=10.10.1.0/25 pref-src=10.10.1.1 gateway=vlan10 gateway-status=vlan10 reachable distance=0 scope=10
 3   ADC  dst-address=10.10.2.0/25 pref-src=10.10.2.1 gateway=vlan20 gateway-status=vlan20 reachable distance=0 scope=10
 4   ADC  dst-address=10.10.3.0/25 pref-src=10.10.3.1 gateway=vlan30 gateway-status=vlan30 reachable distance=0 scope=10
 5   ADC  dst-address=10.10.4.0/25 pref-src=10.10.4.1 gateway=vlan40 gateway-status=vlan40 reachable distance=0 scope=10
 6   ADC  dst-address=10.10.5.0/25 pref-src=10.10.5.1 gateway=vlan50 gateway-status=vlan50 reachable distance=0 scope=10
 7   ADC  dst-address=10.10.6.0/25 pref-src=10.10.6.1 gateway=vlan60 gateway-status=vlan60 reachable distance=0 scope=10
 8   ADC  dst-address=10.10.7.0/25 pref-src=10.10.7.1 gateway=vlan70 gateway-status=vlan70 reachable distance=0 scope=10
```

VOL. 4. NO. 1 AGUSTUS 2018
E-ISSN: 2527-4864

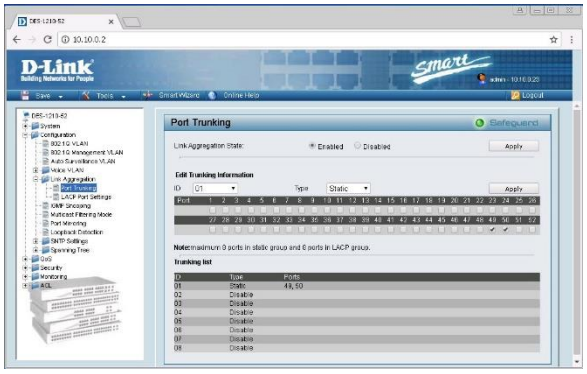
```
9 ADC dst-address=10.10.8.0/25 pref-src=10.10.8.1
gateway=vlan80 gateway-status=vlan80 reachable distance=0
scope=10
10 ADC dst-address=10.10.9.0/25 pref-src=10.10.9.1
gateway=vlan90 gateway-status=vlan90 reachable distance=0
scope=10
11 ADC dst-address=10.10.10.0/25 pref-src=10.10.10.1
gateway=vlan100 gateway-status=vlan100 reachable
distance=0 scope=10
12 ADC dst-address=10.15.15.0/27 pref-src=10.15.15.1
gateway=vlan500 gateway-status=vlan500 reachable
distance=0 scope=10
13 ADC dst-address=192.168.15.0/26 pref-src=192.168.15.1
gateway=vlan600 gateway-status=vlan600 reachable
distance=0 scope=10
14 ADC dst-address=103.3.67.64/29 pref-src=103.3.67.66
gateway=ether1-Wan gateway-status=ether1-Wan reachable
distance=0 scope=10
15 ADC dst-address=172.16.15.0/24 pref-src=172.16.15.254
gateway=vlan200 gateway-status=vlan200 reachable
distance=0 scope=10
```

Jaringan *interface vlan* untuk dapat koneksi ke internet selain routing dibutuhkan juga konfigurasi nat, network address translation pada router MikroTik.

```
[taufik@MT_Kampus] > ip firewall nat pr detail
Flags: X - disabled, I - invalid, D - dynamic
0 ;;; Nat Internet
   chain=srcnat action=masquerade to-addresses=103.3.67.66
out-interface=ether1-Wan log=no log-prefix=""
```

C. Implementasi

Selanjutnya untuk implementasi *vlan* pada Switch Manajemen kampus, membuat Link Aggregation, dengan memilih dua port ethernet(49 dan 50), yang dihubungkan dengan kabel UTP ke router MikroTik

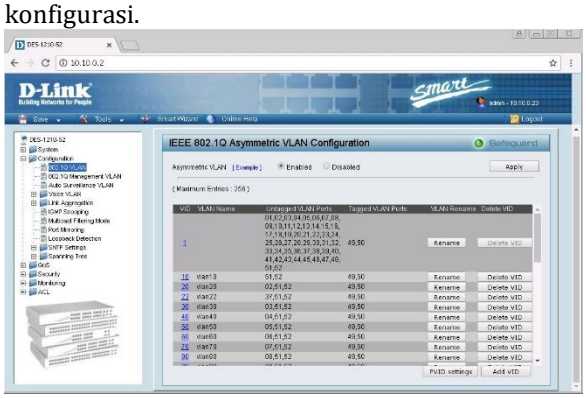


Sumber:(Rahman, 2018)

Gambar 3. Link Aggregation, Port Trunking.

Ada dua tipe link aggregate, port trunking dan LACP. Tetapi yang digunakan pada penelitian ini adalah port trunking tipe statik karena *interface* bonding pada router MikroTik menggunakan mode balance rr.

Langkah selanjutnya konfigurasi *vlan* pada switch manajemen dengan mengaktifkan *vlan* assimetris dahulu, kemudian mengklik add *vlan*, isi *vlan*-id, *vlan*-name, pilih untagged *vlan* ports, tagged *vlan* ports dan klik save untuk menyimpan konfigurasi.



Sumber: (Rahman, 2018)

Gambar 4. Konfigurasi Vlan pada Switch Manajemen

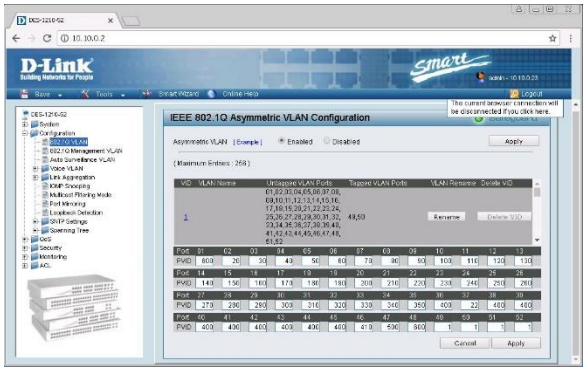
Vlan-ID(VID) adalah identitas unik dari virtual local area network, tidak boleh sama dan mengikuti *vlan*-id yang ada pada router MikroTik atau switch layer-3.

Vlan Name adalah penamaan peruntukan dari *vlan*, misal R201.

Untagged Vlan Ports adalah port *vlan* tak berantai, artinya *vlan* berada di port ini.

Tagged Vlan Ports adalah port yang dilalui oleh *vlan* untuk berkomunikasi.

Port VlanID(PVID) adalah port dimana *vlan*-id ditempatkan.



Sumber:(Rahman, 2018)

Gambar 5. Konfigurasi Port Vlan-ID(PVID)

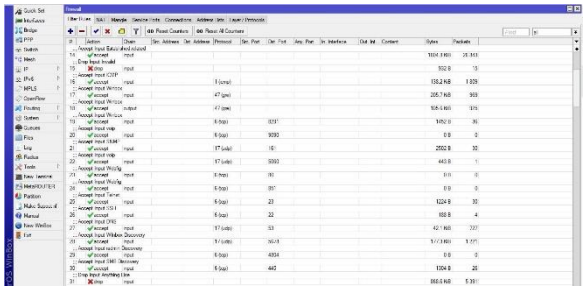
Pada gambar 5, menempatkan *vlan*-id pada port ethernet switch manajemen, sehingga dapat terdokumentasi dan dapat di monitoring penggunaan jaringannya.

Sumber:(Rahman, 2018)

Gambar 6. Monitoring Statistik Port

Setelah konfigurasi PVID, pada gambar 6 penggunaan *vlan* pada port dapat tercatat statistik monitoring penggunaannya, dengan demikian dapat dijadikan bahan untuk evaluasi jika terjadi kerusakan pada port ethernet.

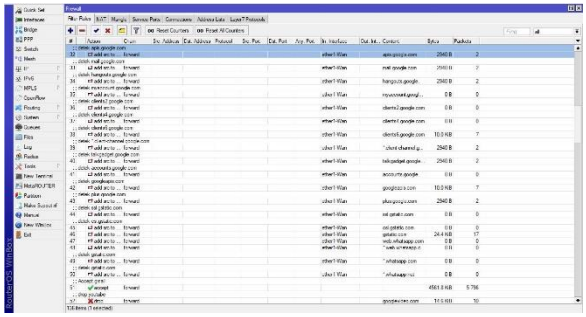
Kebijakan atau policy dari sebuah lembaga atau kampus yang berhubungan dengan penggunaan jaringan di terjemahkan dengan membuat konfigurasi *firewall* pada router MikroTik dibuat dengan model *firewall* bertingkat, artinya dibuka koneksi dengan beberapa port, protokol yang diijinkan selain itu di drop.



Sumber:(Rahman, 2018)

Gambar 7. Firewall Filter Input

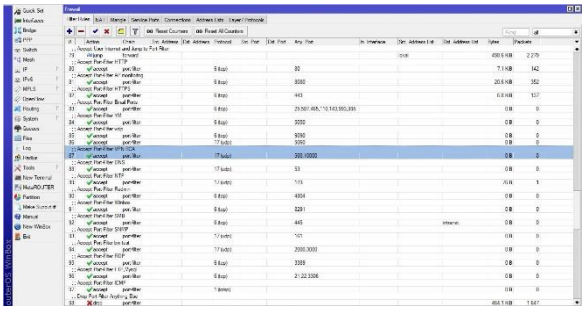
Pada Filter input, membatasi port dan protokol yang boleh melewati router dan masuk ke jaringan di bawah nya. Port yang di accept: 80, 22,23,53,445,8291,9090,161 dan 5060. Untuk protokol: icmp, gre, sedangkan protokol tcp dan udp bergantung pada port yang di accept.



Sumber:(Rahman, 2018)

Gambar 8. Firewall Filter Detek IP

Pada Filter detek ip digunakan untuk menangkap sesuai conten, pada gambar 8 kasus nya adalah tidak boleh akses youtube.com akan tetapi dapat mengakses gmail.com dan Whatsapp. Dengan demikian harus mendeteksi ip yang berhubungan dengan mail google dan Whatsapp. Setelah di tangkap ip tersebut akan di kelompokkan pada address-list diberi nama, misal gmail.



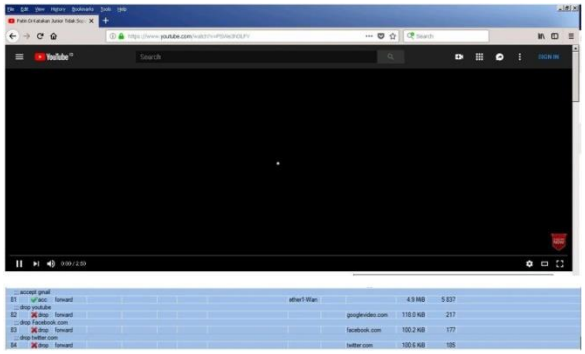
Sumber:(Rahman, 2018)

Gambar 9. Firewall Filter Forward

Bagian akhir dari *firewall* bertingkat adalah *firewall* filter Forward, memilah trafik yang boleh keluar dari jaringan dibawah router berdasarkan protokol, port dan tujuan ip address. Misal port 445 hanya boleh forward ke dst address yang sudah ditentukan, dikonfigurasi sesuai dengan kebutuhan.

D. Testing

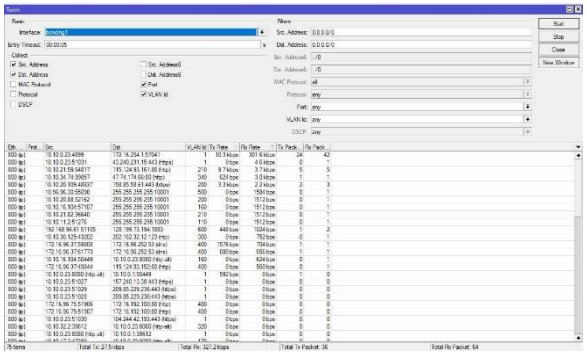
Pada tahap testing yang dilakukan adalah pengujian akses website yang sudah drop pada *firewall* filter yakni youtube, facebook dan twitter dari *interface vlan*1 dengan ip address 10.10.0.23.



Sumber: (Rahman, 2018)

Gambar 10. Test akses youtube

Pada gambar 10, terdapat trafik accept gmail.com juga drop konten googlevideo.com , trafik drop konten facebook.com dan trafik drop konten twitter.com sebagai bukti bahwa rule *firewall* filter berjalan dengan baik.



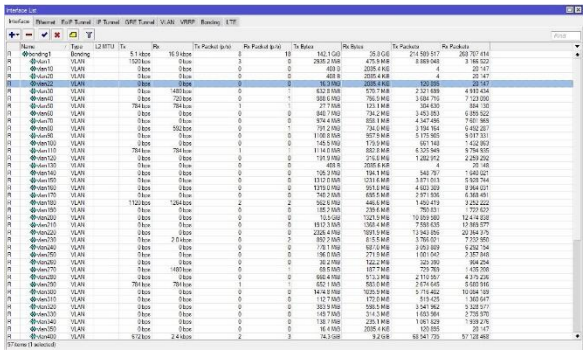
Sumber:(Rahman, 2018)

Gambar 11. Torch Interface Bonding

Dengan menggunakan torch dapat melihat trafik real time. Pada gambar 11, dengan memilih *interface* bonding, dapat dilihat *vlan*-id yang berbeda juga trafik yang sedang berjalan.

E. Manajemen

Tahap manajemen adalah dimana dapat melihat semua atau monitoring trafik dari *interface* virtual local area network



Sumber:(Rahman, 2018)

Gambar 12. Interface list Vlan

Pada gambar 12, adalah hasil dari pada kinerja *interface vlan* berdasarkan tx/rx bytes dan tx/rx packets. Dimana pada *interface* bonding sebagai ujung tumpuan dari semua *interface vlan* memiliki trafik pada Tx byte 142,1GB dan Rx byte 35,8GB. Sedangkan Tx Packets 214589517 dan Rx Packets 268707414, trafik berubah sesuai dengan penggunaan jaringan.

KESIMPULAN

Dengan implementasi *interface vlan* dengan *vlan* id sebagai pembedanya pada router MikroTik pada *interface* bonding, digabungkan nya dua ethernet menjadi satu menggunakan mode balance rr, maka dapat memisahkan trafik jaringan sehingga broadcast dari pada jaringan dapat diminimalisir dan menjadi mudah dalam memantau trafik penggunaan jaringan, mendeteksi kegagalan koneksi dapat ditelusuri berdasarkan PVID melalui monitoring switch manajemen. Kebijakan mengenai penggunaan jaringan diimplementasikan menggunakan *firewall* pada router MikroTik kampus sehingga dapat di monitoring trafik dan paket data yang masuk dan keluar. Hal ini di buktikan dengan beberapa website yang tidak dapat diakses, begitupun dengan port dan protokol jaringan.

REFERENSI

Ali, M. N. Bin, Rahman, M. L., & Hossain, S. A. (2013). Network architecture and security issues in campus networks. *2013 4th International Conference on Computing, Communications and Networking Technologies, ICCCNT 2013*, 1–9. https://doi.org/10.1109/ICCCNT.2013.6726595

Hameed, A., & Mian, A. N. (2015). Towards better traffic localization of virtual lans using genetic algorithm. *Computer Journal*, *59*(2), 178–191. https://doi.org/10.1093/comjnl/bxv088

Kodama, S., Nakagawa, R., Tanouchi, T., & Kameyama, S. (2016). Management system by using embedded packet for hierarchical local area network. *2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 1–4. https://doi.org/10.1109/UEMCON.2016.7777868

Lehocine, M. B., & Batouche, M. (2017). Flexibility of managing VLAN filtering and segmentation in SDN networks. *2017 International Symposium on Networks, Computers and Communications, ISNCC 2017*. https://doi.org/10.1109/ISNCC.2017.8071999

Pauzhi, W., & Coronel, J. (2015). Security for WISP through Mikrotik equipment Mikrotik). In *2015 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)* (pp. 229–233). Santiago, Chile.

Rahman, T. (2018). Laporan Akhir Penelitian Mandiri. Jakarta: AMIK BSI Jakarta.

Rianafirin, K., & Kurniawan, M. T. (2017). Design Network Security Infrastructure Cabling Using Network Development Life Cycle Methodology and ISO/IEC 27000 Series in Yayasan Kesehatan (Yakes) Telkom

Bandung. In *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)* (pp. 1–6). Kuta Bali, Indonesia: IEEE. Retrieved from https://ieeexplore.ieee.org/document/8320681/

Wiboonrat, M. (2014). Data center infrastructure management: WLAN networks for monitoring and controlling systems. *International Conference on Information Networking*, 226–231. https://doi.org/10.1109/ICOIN.2014.6799696

Zhou, J., & Ma, Y. (2016). Topology discovery algorithm for ethernet networks with incomplete information based on VLAN. *Proceedings of 2016 5th International Conference on Network Infrastructure and Digital Content, IEEE IC-NIDC 2016*, 396–400. https://doi.org/10.1109/ICNIDC.2016.7974604