BAB III
METODE PENELITIAN

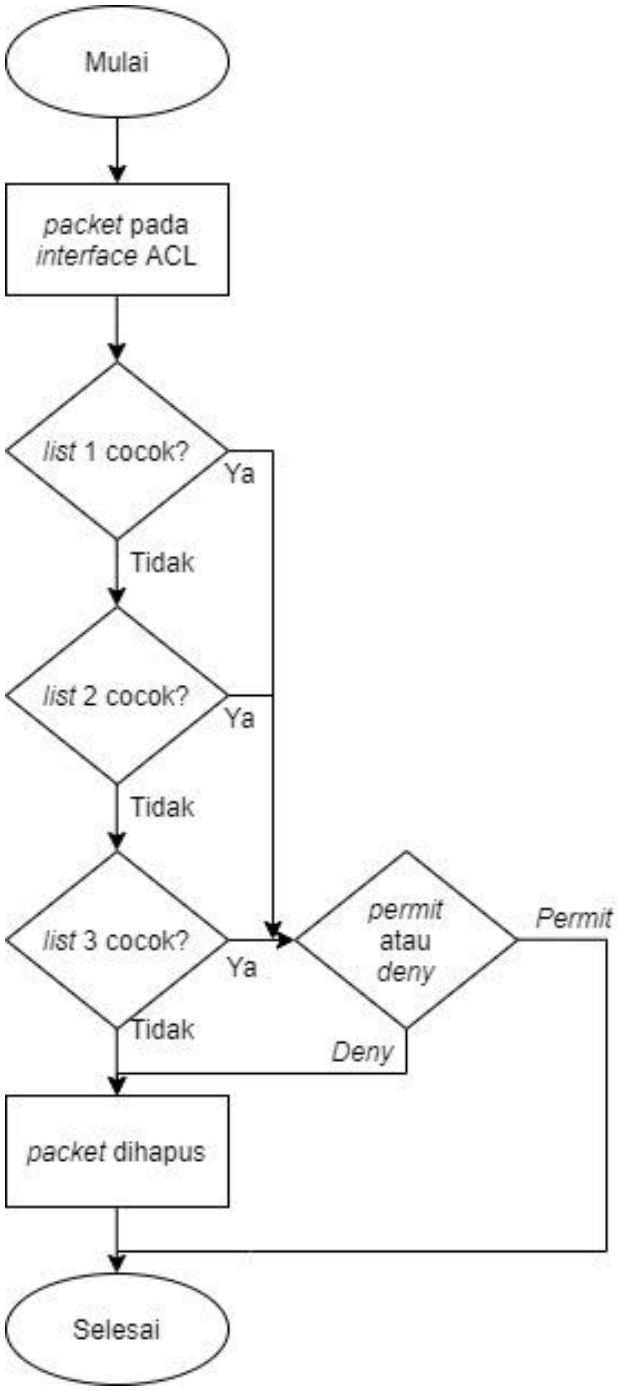
3.1 Tahapan Penelitian

Pada tahapan penelitian ini penulis akan menguraikan seluruh proses penelitian kegiatan selama penelitian berlangsung. Adapun tahapan penelitian yang dilakukan terdapat pada bagan alir gambar 3.1

Gambar 3.1 Alur penelitian

3.1.1 ALUR SKENARIO JARINGAN

Pada gambar 3.2 menjelaskan alur skenario jaringan, di mana ketika sebuah paket dikirimkan dan melewati *interface* yang sudah diterapkan ACL maka paket akan dicek dan dicocokan dengan *list* yang sudah dibuat, di mana pencocokan dilakukan secara *squential* yaitu berurut dari atas ke bawah.



Gambar 3.2 Alur Skenario Jaringan

Saat ACL cocok pada *list* pertama maka akan dilanjutkan sesuai perintah *deny* atau *permit,* jika perintahnya *permit* maka akan langsung dikirimkan ketujuan sesuai dengan jalur yang ada pada tabel *routing* sedangkan saat perintahnya *deny* maka paket akan dihapus/dibuang. Ketika aturan pertama tidak cocok maka akan berlanjut ke *list* kedua cara kerjanya sama seperti sebelumnya yaitu saat ACL cocok pada *list* maka akan dilanjutkan sesuai perintah *deny* atau *permit,* jika perintahnya *permit* maka akan langsung dikirimkan ketujuan sesuai dengan jalur yang ada pada tabel *routing* sedangkan saat perintahnya *deny* maka paket akan dihapus/dibuang. Ketika aturan pertama dan kedua tidak cocok maka akan dilanjutkan pada aturan ketiga, ketika *list* cocok maka akan dilanjutkan sesuai perintah untuk melakukan *permit* atau *deny.* Jika perintahnya *permit* maka akan langsung dikirimkan ketujuan sesuai dengan jalur yang ada pada tabel *routing* sedangkan saat perintahnya *deny* maka paket akan dihapus/dibuang.

3.1.2 STUDI LITERATUR

Pada tahapan ini penulis melakukan studi literatur dengan mencari sumber-sumber teori yang berkaitan dengan pembahasan penelitian yang akan dilakukan. Sumber-sumber teori yang menjadi pendukung teori didapatkan melalui buku, jurnal dan *website* yang membahas mengenai topik penelitian. Berdasarkan sumber-sumber yang telah didapatkan maka penulis dapat merancang dan melakukan tahap-tahap dalam penelitian.

3.1.3 ANALISA KEBUTUHAN

Pada tahapan ini, penulis dapat menentukan kebutuhan apa saja yang diperlukan untuk melakukan proses penelitian. Dalam penelitian ini ada dua jenis perangkat yang digunakan dalam penelitian yaitu perangkat keras (*hardware*) dan perangkat lunak (*software*). Dari hasil studi literatur yang sudah dilakukan penulis dapat menentukan perangkat-perangkat dan hal apa saja yang akan digunakan dalam penelitian.

3.1.4 PERANGKAT

Pada penelitian ini, penulis membutuhkan perangkat-perangkat dalam melakukan penelitian yang terdiri dari perangkat keras (*hardware*) dan perangkat lunak (*software*), yaitu:

a. Perangkat Keras (*Hardware*)

Perangkat keras yang digunakan dalam penelitan terdapat dalam table 3.1.

Tabel 3.1 Perangkat Keras (*Hardware*)

Nama	Tipe/Spesifikasi	Jumlah
Laptop	Acer Aspire E5-476G, Windows 10, RAM 8 GB, IntelI Core™ i3-8130U	1
Router (Mikrotik)	Mikrotik-6.45.9	1
Multilayer Switch	Cisco ios 3725 (Dynamips)	1
Switch Layer 2	Cisco Vios	3
PC (VPCS)		6

b. Perangkat Lunak (*Software*)

Pada penelitian ini selain perangkat keras penulis juga membutuhkan perangkat lunak yang terdapat pada gambar 3.2.

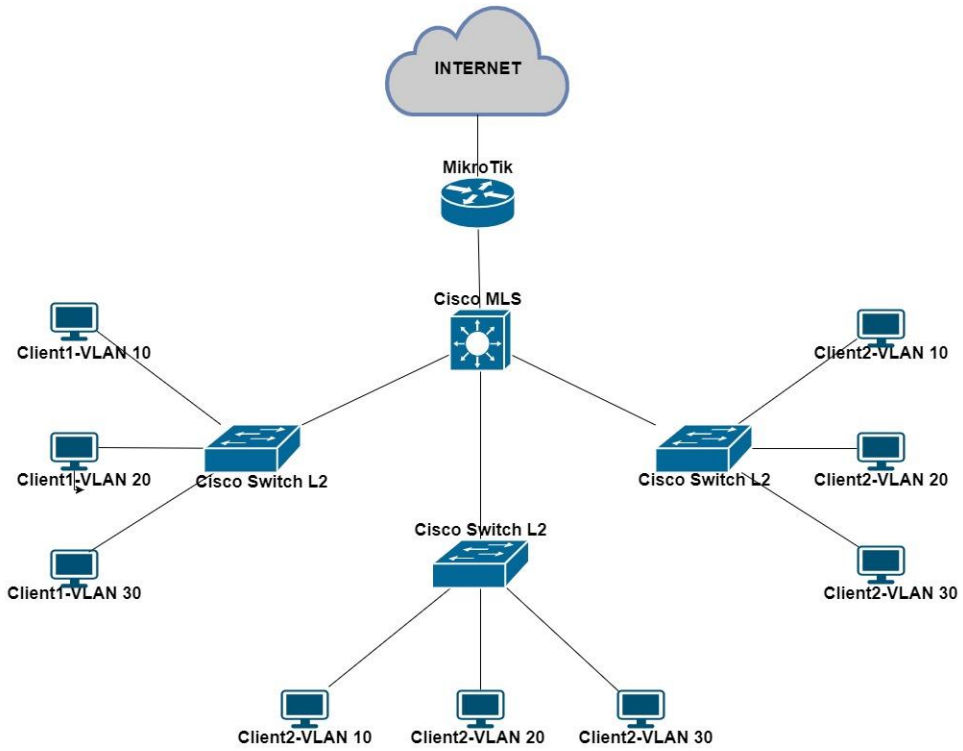
Tabel 3.2 Perangkat Lunak (*Software*)

Nama	Deskripsi	Jumlah
Windows 7 (32-bit)	OS untuk *client* pada vlan 10	1
Ubuntu 18.04	OS untuk *client* pada vlan 20 dan 30	2
GNS3	Simulator pembangunan jaringan	1
SolarWinds	Tool untuk telnet perangkat	1
VirtualBox	VM untuk GNS3 dan Perangkat Jaringan	1
Cisco IOS 3725	OS untuk *Multilayer Switch*	1
Cisco IOS i86bi-linux-l2-adventerprisek9-15.1a	OS untuk *switch layer* 2	3
Mikrotik OS chr-6.49.4	OS untuk router mikrotik sebagai *core* router	1

3.1.5 TOPOLOGI JARINGAN

Topologi jaringan yang dirancang terdiri dari satu buah *router* mikrotik yang digunakan sebagai *core router* sekaligus *router* yang

digunakan sebagai NAT untuk komunikasi jaringan lokal dan publik. Satu buah *multilayerswitch* milik cisco yang digunakan sebagai VTP (*Vlan Trunking Protocol*) server guna menyebarkan vlan beserta konfigurasinya kepada VTP *client* dan juga akan difungsikan untuk konfigurasi *Access Control List* yang akan membatasi jaringan antar VLAN yang berbeda maupun akses jaringan VLAN terhadap jaringan Publik.



Gambar 3.3 Topologi Jaringan

Kemudian terdapat tiga buah *switch* yang berfungsi sebagai *layer* 2 *switch* dan sebagai VTP *client* guna menerima konfigurasi VLAN dari VTP server yang terkoneksi dengan *multilayer switch*/VTP server melalui *port trunk* dan untuk akses kepada *end-device* (PC). Kemudian terdapat 9 buah PC di mana 1 menggunakan OS Windows 7 yang terletak pada VLAN 10, 2 OS Ubuntu 18.04 pada VLAN 20 dan VLAN 30 (VLAN lokal) serta 6 lainya menggunakan VPCS yang mana VLAN 20 dan VLAN 20 akan difungsikan sebagai koneksi lokal saja. Adapun topologi yang dirancang terdapat pada gambar 3.3.

Pada penelitian ini, selain perangkat yang dibutuhkan penulis juga perlu memberi alamat IP pada tiap-tiap perangkat. Alamat IP perangkat dapat dilihat pada tabel 3.3.

Tabel 3.3 Alamat IP Perangkat

No	Perangkat	Interface	Alamat IP
1	Internet	-	192.168.137.1/24
2	Router MikroTik	Ether1	192.168.137.10/24
		Ether2	10.10.10.1/30
3	Cisco Multilayer Switch	Ether 1/0	10.10.10.2/30
		VLAN 10	192.168.10.1/24
		VLAN 20	192.168.20.1/24
		VLAN 30	192.168.30.1/24
4	Client1-VLAN10	Ether0	192.168.10.10/24
5	Client1-VLAN20	Ether0	192.168.20.10/24
6	Client1-VLAN30	Ether0	192.168.30.10/24
7	Client2-VLAN10	Ether0	192.168.10.20/24
8	Client2-VLAN20	Ether0	192.168.20.20/24
9	Client2-VLAN30	Ether0	192.168.30.20/24
10	Client3-VLAN10	Ether0	192.168.10.30/24
11	Client3-VLAN20	Ether0	192.168.20.30/24
12	Client3-VLAN30	Ether0	192.168.30.30/24

Alamat IP yang digunakan merupakan alamat yang digunakan untuk komunikasi antara perangkat agar dapat terhubung dan berkomunikasi. Router mikrotik yang berfungsi sebagai *core router* merupakan penghubung antara jaringan publik dan jaringan lokal, pada *multilayer switch* terdapat 3 buah VLAN dengan alamat IP yang berbeda di mana VLAN 20 dan 30 akan difungsikan sebagai jaringan lokal yang tidak dapat berkomunikasi dengan VLAN 10 maupun dengan jaringan publik maka perlu adanya dikonfigurasi *Acces Control List* sebagai *filtering*-nya yang dilakukan saat ACL sebelum dan sesudah diterapkan. Kemudian akan dilakukan pengujian QoS untuk mengetahui perfomansi dari jaringan. Selanjutnya akan dilakukan analisa terhadap jaringan sebelum dan sesudah ACL diterapkan.

3.1.6 KONFIGURASI *RULES*

Pada tahapan ini, perangkat yang sudah dipersiapkan selanjutnya akan dikonfigurasi sebelum dilakukanya tahap pengujian. Tahapan konfigurasi yang akan dilakukan adalah:

3.1.6.1 Konfigurasi *Router* Mikrotik

a. Konfigurasi IP *Address*

Pada tahap konfigurasi IP *address* terdapat dua IP *address* pada *interface* yang digunakan, yaitu *interface* ether1 yang mengarah pada internet dan ether2 yang mengarah dan difungsikan untuk jaringan lokal.

```
Ip address add address=192.168.137.10/24 interface=ether1
comment=INTERNET

Ip address add address=10.10.10.1/30 interface=ether2
comment=LOCAL
```

Pada tampilan konfigurasi ip *address* di atas terlihat bahwa *interface* ether1 digunakan sebagai *interface* yang mengarah ke jaringan publik/internet sedangkan pada *interface* ether2 merupakan *interface* yang digunakan dan mengarah ke jaringan lokal.

```
[admin@MikroTik] > ip address print
Flags: X - disable, I - Invalid, D -dynamic
#     ADDRESS              NETWORK             INTERFACE
0     ;;; INTERNET
      192.168.137.10/24    192.168.137.0       ether1
1     ;;; LOCAL
      10.10.10.1/30        10.10.10.0          ether2
```

Setelah tahap konfigurasi IP *address* selesai dilakukan, penulis melakukan verifikasi terhadapat IP *address* yang telah dikonfigurasi untuk memastikan apakah IP *address* sudah terkonfigurasi dengan benar. Dapat dilihat pada tampilan hasil konfigurasi di atas bahwa *interface* ether1 sudah berhasil terkonfigurasi IP *address* dengan koment internet begitupun juga pada *interface* ether2 sudah terkonfigurasi IP *address* dengan komen *local*.

b. Konfigurasi *Gateway*

Konfigurasi *gateway* dilakukan agar perangkat pada jaringan lokal dapat terhubung dengan jaringan internet/publik, untuk itu perlu adanya konfigurasi *gateway* sebagai pintu keluar dan masuk terhadapap jaringan publik, *gateway* pada router dikonfigurasi menggunakan alamat IP yang diberikan oleh sebuah *Internet Service Provider* (ISP) berupa IP publik, dengan mengetikan perintah “ip router add gateway=(alamat ip ISP) maka

router mikrotik sudah dapat terkoneksi dengan internet. Perintah konfigurasi sebagai berikut:

```
[admin@MikroTik] > ip route add gateway=192.168.137.1
cooment=Gateway
```

Hasil konfigurasi dapat di lihat pada tampilan dibawah, dalam router mikrotik *gateway* sudah terkonfigurasi, dengan lambang A-S yang berarti *Activ-Static* atau terkonfigurasi secara *static*/manual, dengan alamat tujuan menggunakan *defaulth route* yang berarti semua *network* yang terhubung akan menggunakan *gateway* yang terkonfigurasi menggunakan alamat IP ISP.

```
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect,
S - static,
B - blackhole, U - unreachable, P - prohibit
#     DST-ADDRESS     PREF-SRC         GATEWAY       DISTANCE
0 A S ;;; Gateway
      0.0.0.0/0                        192.168.137.1        1
1 ADC 10.10.10.0/30   10.10.10.1       ether2               0
2 ADC 192.168.137.0   192.168.137.10   ether1               0
```

c. *Routing Static*

Routing static merupakan proses menambahkan jalur perutean secara manual agar alamat IP *address* yang berbeda *network* dapat terhubung satu sama lain. Secara *default* pada *router* mikrotik akan membuat *routing dynamic* ketika IP *Address* terkonfigurasi pada *interface* mikrotik.

```
Ip route add dst-address=192.168.10.0/24 gateway
10.10.10.2
Ip route add dst-address=192.168.20.0/24 gateway
10.10.10.2
Ip route add dst-address=192.168.30.0/24 gateway
10.10.10.2
```

Pada tampilan konfigurasi *static route* di atas, alamat *network* yang terdaftar merupakan alamat yang akan digunakan dalam VLAN 10, VLAN 20 dan VLAN 30 dengan *gateway* yang diberikan merupakan IP *address* dari router

tetangga yaitu IP *address* pada *multilayer switch* yang berfungsi sebagai *interface* keluaran untuk alamat *network* pada VLAN.

d. Konfigurasi *Network Address Translation* (NAT)

Network Address Translation (NAT) memungkinkan untuk banyak IP Addres pada jaringan lokal dapat terhubung dengan jaringan publik/internet hanya dengan menggunakan satu alamat IP *Address* saja. NAT memungkinkan untuk perangkat komputer yang memiliki alamat IP *private* untuk dapat terhubung dengan internet, karena perangkat yang tidak memilik IP publik tidak akan terhubung ke internet jika tidak melalui NAT ini.

```
[admin@Mikrotik] > ip firewall nat add cahin=srcnat
action=masquerade out-interface=ether1
```

Pada tampilan konfigurasi NAT di atas terdapat *chain* yang merupakan proses yang dialamai oleh paket, dilanjutkan dengan (*action*) adalah aksi yang akan dialami oleh sebuah paket, aksi yang digunakan merupakan (*masquerade*) yang berfungsi sebagai translasi untuk IP lokal (*private*) agar dapat terhubung dengan jaringan internet (*public*) dengan *interface* keluaran yang ditetapkan adalah ether1.

e. Mengamankan *Router* MikroTik

Dalam membangun sebuah jaringan tentu hal yang snagat penting adalah keamanan dari sebuah router itu sendiri.

```
[admin@MikroTik]>ip service disable
telnet,ftp,www,api,api-ssl,www-ssl
[admin@MikroTik]>ip service set ssh port=1212
[admin@MikroTik]>ip service set winbox port=2121
[admin@MikroTik]>tool mac-server set allowed-interface-
list=none
[admin@MikroTik]>tool mac-server ping set enabled=no
[admin@MikroTik]>tool bandwitch-server set enabled=no
[admin@MikroTik]>ip dns set allow-remote-request=no
[admin@MikroTik]>ip proxy set enabled=no
[admin@MikroTik]>ip socks set enabled=no
[admin@MikroTik]>ip upnp set enabled=no
[admin@MikroTik]>ip ssh set strong-crypto=yes
```

disalahgunakan dari pihak luar yang tidak bertanggung jawab. *Service-service* pada router mikrotik secara *defaulth* akan aktif oleh sebab itu perlu adanya pengamanan terhadap *port* dan *service-service* yang tidak

diperlukan dalam router mikrotik. Penulis mengamankan router mikrotik seperti pada tampilan di atas, terlihat bahwa *service log in* yang digunakan melalui telnet, ftp, www, api, api-ssl dan www-ssl telah *disable* agar *log in* yang dilakukan tidak dapat melalui fitur tersebut, kemudian untuk mencegah akses malului *port* ssh dan telnet maka perlu adanya perubahhan nomor *port* dan diikuti *service-service* lainya yang dibutuhkan untuk keamanan router.

3.1.6.2 KONFIGURASI *MULTILAYERSWITCH*

Pada tahap ini perangkat *multilayer switch* akan dikonfigurasi VTP-Server sebagai pusat untuk konfigurasi VLAN dan menyebarkan VLAN tersebut, *multilayerswitch* nantinya akan dikonfigurasi *Access Control List* untuk membatasi antar jaringan VLAN satu dengan yang lain.

1) Konfigurasi IP *Address*

Multilayerswich perlu adanya konfigurasi IP *address* agar jaringan lokal dapat terhubung dengan jaringan internet yang sudah terkonfigurasi pada mikrotik, adapun konfigurasi IP *address* pada *multilayerswitch* terdapat pada perintah:

```
MLS(config)#int e0/0
MLS(config-if)#description MLS-MikroTik
MLS(config-if)#no switchport
MLS(config-if)#ip address 10.10.10.2 255.255.255.252
MLS(config-if)#no shutdown
```

Pada tampilan konfigurasi di atas terlihat bahwa *interface* yang terhubung langsung dengan mikrotik yaitu e0/0 di mana ini merupakan jembatan penghubung untuk membangun konektivitas diantara keduanya, agar konektivitas dapat terjadi maka konfigurasi IP *Address* perlu dilakukan, IP *address* yang dikonfigurasi harus satu network dengan router MikroTik agar dapat terhubung satu sama lain.

2) Konfigurasi VLAN

Pada tahap ini VLAN yang dikonfigurasi pada *multilayer switch* akan berfungsi sebagai *gateway* untuk tiap *host* vlan yang terdiri dari VLAN 10, VLAN 20 dan VLAN 30.

```
MLS(config)#interface vlan 10
MLS(config-if)#ip address 192.168.10.1 255.255.255.0
MLS(config)#interface vlan 20
MLS(config-if)#ip address 192.168.20.1 255.255.255.0
MLS(config)#interface vlan 30
MLS(config-if)#ip address 192.168.30.1 255.255.255.0
```

Konfigurasi VLAN dilakukan agar *host* pada VLAN nantinya mempunyai alamat IP tersendiri. Pada tampilan konfigurasi di atas terdapat 3 buah VLAN dengan *network* yang berbeda, di mana VAN 20 dan 30 (VLAN lokal) nantinya akan difungsikan sebagai koneksi lokal saja sedangkan VLAN 10 akan dapat bebas sepenuhnya mengakses jaringan publik.

3) VTP-Server

Mutilayerswitch pada penelitian ini juga berfungsi sebagai VTP-Server di mana VLAN dan konfigurasi yang ada pada *multilayerswitch* akan disebarkan kepada *switct-switch* lain yang berfungsi sebagai VTP-*Client.* Konfigurasi VTP-server dapat dilihat pada konfigurasi dibawah :

```
MLS(config)#vtp mode server
MLS(config)# domain nanda
MLS(config)#vtp password 12345
MLS(config)#vtp version 2
```

Pada tahapan ini *multilayerswitch* perlu diatur/*setting* dengan mode server kemudian perlu adanya penamaan domain dan *password*, agar perangkat *switch* yang berfungsi sebagai VTP-*Client* ketika mengatur domain dan *password* yang sama dapat terhubung dan menerima konfigurasi yang disebar melalui VTP-Server.

4) Konfigurasi *Defaulth Gateway* MLS

Pada tahapan ini *defaulth gateway* akan dikonfigurasi pada *mutilayerswitch* sebagai perangkat utama yang digunakan untuk *client,* dengan adanya

```
MLS(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.1
```

dapat terhubung ke publik melalui router mikrotik sebagai *defaulth gateway*nya.

Pada tampilan konfigurasi ip *route* di atas terlihat bahwa ip *route* dengan *network* yang diberikan yaitu 0.0.0.0 0.0.0.0 merupakan semua *network* yang terhubung dengan perangkat *multilayerswitch* akan terhubung dengan

gateway 10.10.10.1 pada router mikrtotik, dengan adanya proses *routing* ini maka jaringan lokal akan dapat terhubung dengan jaringan publik.

3.1.6.3 *SWITCH LAYER* 2

Pada tahap ini *switch layer* 2 akan difungsikan sebagai VTP-*Client*, diamana pada *switch layer* 2 tidak perlu untuk konfigurasi VLAN dan hanya perlu mengatur *switch layer* 2 menjadi VTP-*Client* agar VLAN dan konfigurasi yang ada dapat diterima dari yang sebarkan melalui *multilayer switch* (VTP-Server).

```
SWITCH-2(config)#vtp mode client
SWITCH-2(config)#vtp domain nanda
SWITCH-2(config)#vtp password 12345
SWITCH-2(config)#interface e0/0
SWITCH-2(config-if)#switchport trunk encapsulation dot1q
SWITCH-2(config-if)#switchport mode trunk
```

Pada tampilan konfigurasi di atas dapat dilihat bahwa perangkat *switch* akan di atur menjadi mode *client*, kemudian dengan alamat domain serta *password* yang sama pada VTP-server, dengan ini maka VTP-*Client* dapat menerima VLAN beserta konfigurasinya yang telah disebarkan melalui VTP-Server, tidak hanya itu saja penulis juga mengkonfigurasi untuk *interface* yang terhubung dengan *multilayerswitch* (VTP-Server) dengan set ke mode *trunk* hal ini perlu dilakukan karena VLAN-VLAN dalam VTP dapat tersebar jika mealui *port trunk* saja. Selain itu perlu adanya konfigurasi *port access* untuk menuju ke *end-device*, adapun perintahnya:

```
SWITCH-2(config-if)#interface e1/1
SWITCH-2(config-if)#switchport mode access
SWITCH-2(config-if)#switchport access vlan 10
SWITCH-2(config-if)#interface e1/1
SWITCH-2(config-if)#switchport mode access
SWITCH-2(config-if)#switchport access vlan 10
SWITCH-2(config-if)#interface e1/1
SWITCH-2(config-if)#switchport mode access
SWITCH-2(config-if)#switchport access vlan 10
```

dengan *end-device* untuk menunjukan perangkat *end-device* termasuk golongan ke dalam VLAN berapa. Pada tampilan konfigurasi di atas terlihat bahwa terdapat 3 *interface* yang berbeda kemudian diatur ke mode *access*, setelah itu pada *interface* yang dipilih akan diberikan akses VLAN yang sesuai dengan topologi.

3.1.7 *ACCESS CONTROL LIST*

Pada tahapan ini merupakan tahapan inti yang akan berperan sebagai pembatasan hak akses antara *network* pada masing VLAN dan juga pembatasan akses terhadap jaringan VLAN yang akan digunakan sebagai koneksi lokal saja untuk tidak dapat terhubung dengan jaringan publik/internet.

```
MLS(config)# access-list 100 deny ip 192.168.20.0
0.0.0.255 192.168.10.0 0.0.0.255
MLS#access-list 100 permit ip 192.168.20.0 0.0.0.255 any
MLS(config)# int vlan 20
MLS(config-if) ip access-group 100 in
MLS(config)#access-list 110 deny ip 192.168.30.0
0.0.0.255 192.168.10.0 0.0.0.255
MLS(config)#access-list 110 permit ip 192.168.30.0
0.0.0.255 any
MLS(config)# int vlan 30
MLS(config-if) ip access-group 110 in
MLS(config)#access-list 120 deny ip 192.168.10.0
0.0.0.255 192.168.20.0 0.0.0.255
MLS(config)#access-list 120 deny ip 192.168.10.0
0.0.0.255 192.168.20.0 0.0.0.255
MLS(config)#access-list 120 permit ip 192.168.10.0
0.0.0.255 any
MLS(config)# int vlan 10
MLS(config-if) ip access-group 120 in
MLS(config)#access-list 10 deny ip 192.168.20.0 0.0.0.255
MLS(config)#access-list 10 deny ip 192.168.20.0 0.0.0.255
MLS(config)#access-list 10 permit any
MLS(config)#int e0/0
MLS(config-if)#ip access-group 10 out
```

Pada tampilan konfigurasi *access-list* di atas terdapat 4 nomor ACL, di mana terdapat dua jenis ACL yang berbeda yaitu *extended* dan *standard. Extended* ACL dengan nomor 100 yang akan diterapkan pada *interface* VLAN 30 berfungsi untuk melakukan *filtering* pada VLAN 10 terhadap VLAN 30, selanjutnya nomor ACL 110 akan diterapkan pada VLAN 20 yang berfungsi untuk melakukan *filtering* jaringan pada VLAN 10 terhadap VLAN 20 kemudian pada nomor ACL 120 akan diterapkan pada *interface* VLAN 10 yang akan melakukan *filtering* jaringan untuk VLAN 20 dan VLAN 30 terhadap VLAN 10. Sedangkan untuk *standard* ACL dengan nomor 10 berfungsi untuk melakukan *filtering* pada VLAN 20 dan VLAN 30 (VLAN lokal) terhadap jaringan publik (internet).

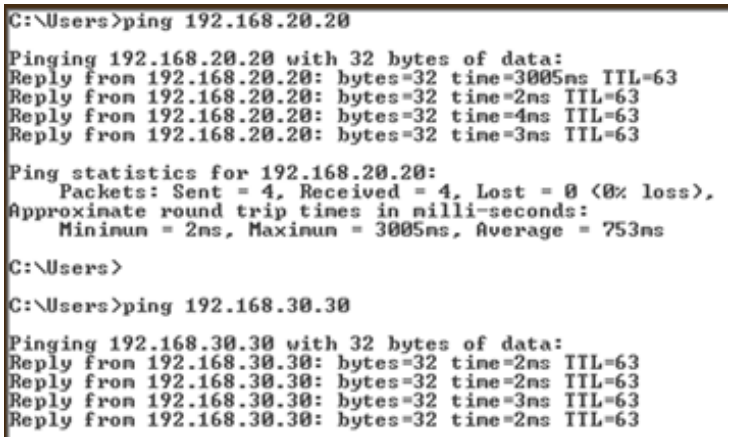
3.1.8 PENGUJIAN KONEKTIVITAS JARINGAN

Pada tahap ini penulis melakukan pengujian terhadap konektivitas jaringan vlan 10 dan vlan lokal terhadap jaringan publik dengan melakukan *streaming* vidio, sedangkan untuk pengujian konektivitas pada jaringan vlan lokal terhadap vlan 10 serta untuk pengujian konektivitas pada vlan lokal dilakukan dengan melakukan *ping* dengan beban yang dibawa sebesar 12.800 *Bytes* (100 bps) dan dilakukan selama 30 kali percobaan. Pengujian konektivitas dilakukan dengan 2 skenario yang berbeda, yaitu skenario 1 saat sebelum *Access Control List* diterapkan dan skenario 2 saat *Access Control List* sudah diterapkan. untuk mengetahui bagaimana ACL dalam membatasi suatu jaringan terhadap jaringan yang di *filter* serta untuk mengetahui pengaruh terhadap konektivitas jaringan vlan yang lainnya. Tabel pengujian dalam penilitian dapat dilihat pada tabel 3.4.

Tabel 3.4 Skenario Pengujian Konektivitas Pada Jaringan

Konektivitas	**Skenario**	**Beban (Bps)**	**Percobaan**
Vlan Lokal - publik	Skenario 1	100	30
	Skenario 2	100	30
Vlan 10 – publik	Skenario 1	100	30
	Skenario 2	100	30
Vlan lokal – Vlan 10	Skenario 1	100	30
	Skenario 2	100	30
Vlan Lokal	Skenario 1	100	30
	Skenario 2	100	30

Pada pengujian konektivitas, dilakukan dengan cara mengirimkan *packet* ICMP antara jaringan vlan yang berbeda sedangkan untuk pengujian konketivitas terhadap jaringan publik dilakukan dengan cara menonton vidio *streaming* pada *youtube.*



Gambar 3.4 Pengujian Konektivitas Sebelum ACL Diterapkan

Pada gambar 3.4 terlihat bahwa dari hasil pengujian konektivitas yang dilakukan sebelum ACL diterapkan akan mendapatkan hasil berupa *replay* yang berasal dari tujuan (*destination*) dengan mengirimkan sebuah *packet* ICMP (*ping*), hal ini menunjukan bahwa konektivitas kedua jaringan tersebut dapat mengirim dan menerima paket secara normal.

```
root@PC:~# ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.
From 192.168.30.1 icmp_seq=1 Packet filtered
From 192.168.30.1 icmp_seq=2 Packet filtered
From 192.168.30.1 icmp_seq=3 Packet filtered
From 192.168.30.1 icmp_seq=4 Packet filtered
^C
--- 192.168.10.10 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet

root@PC:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 192.168.30.1 icmp_seq=1 Packet filtered
From 192.168.30.1 icmp_seq=2 Packet filtered
From 192.168.30.1 icmp_seq=3 Packet filtered
From 192.168.30.1 icmp_seq=4 Packet filtered
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet
```

Gambar 3.5 Pengujian ACL Setelah ACL Diterapkan

Pada pengujian konektivitas selanjutnya merupakan pengujian di mana *Access Control List* telah diterapkan, dapat dilihat pada gambar 3.5 bahwa setelah adanya pemblokiran jaringan yang berfungsi untuk menghindari konektivitas terhadap jaringan yang tidak bisa di akses maka saat mengirimkan sebuah paket ICMP akan muncul tulisan "*packet filtered*" atau "*communication administratively prohibited*" di mana *output* yang dihasilkan merupakan pemberitahuan bahwa konektivitas telah dilarang

atau dibatasi, untuk dapat membukanya hanya administrator jaringan yang mempunyai kewenangan yang dapat membuka jalur antara keduanya.

3.1.9 Analisa Hasil

Pada tahap ini, penulis melakukan dua analisis komparatif dari kedua skenario, yaitu saat *Access Control List* sudah diterapkan dan saat *Access Control List* sebelum diterapkan. Metode yang digunakan dalam mengukur perfomansi suatu jaringan adalah *Quality Of Service* (QOS). Beberapa parameter QoS yang akan diukur berupa *delay, jitter, packet loss* dan *throughput*.

1. *Throughput*

   Pengukuran nilai *throughput* yang sesuai dengan standarisasi *Telecommunications and Internet Protocol Over Networks* (TIPHON) memiliki bebrapa pembagian kategori untuk menuntukan kualitasi seperti pada tabel 3.5.

Tabel 3.5 Standar Kualitas *Throughput*[29]

Kategori *Throughput*	Nilai *Throughput* (bps)	Indeks
Sangat Baik	>100	4
Baik	75	3
Cukup Baik	50	2
Buruk	<25	1

2. *Delay*

   Pengukuran nilai *delay* yang sesuai dengan standarisasi *Telecommunications and Internet Protocol Over Networks* (TIPHON) memiliki bebrapa pembagian kategori untuk menuntukan kualitasi seperti pada tabel 3.6.

Tabel 3.6 Standar Kualitas Delay[29]

Kategori *Latency*	Nilai *Delay* (ms)	Indeks
Sangat Baik	<150 ms	4
Baik	150 ms s/d 300 ms	3
Cukup Baik	300 s/d 450 ms	2
Buruk	>450 ms	1

3. *Jitter*

Pengukuran nilai *jitter* yang sesuai dengan standarisasi *Telecommunications and Internet Protocol Over Networks* (TIPHON) memiliki bebrapa pembagian kategori untuk menuntukan kualitasi seperti pada tabel 3.7.

Tabel 3.7 Standar Kualitas *Jitter*[29]

Kategori *Latency*	*Peak Jitter* (ms)	Indeks
Sangat Baik	0 ms	4
Baik	1 s/d 75 ms	3
Cukup Baik	76 s/d 125 ms	2
Buruk	>225 ms	1

4. *Packet Loss*

Pengukuran nilai jitter yang sesuai dengan standarisasi *Telecommunications and Internet Protocol Over Networks* (TIPHON) memiliki bebrapa pembagian kategori untuk menuntukan kualitasi seperti pada tabel 3.8.

Tabel 3.8 Standar Kualitas *Packet Loss*[29]

Kategori *Degredasi*	Nilai *Packet Loss* (%)	Indeks
Sangat Baik	0 – 2%	4
Baik	3 - 14%	3
Cukup Baik	15 - 24%	2
Buruk	>25%	1