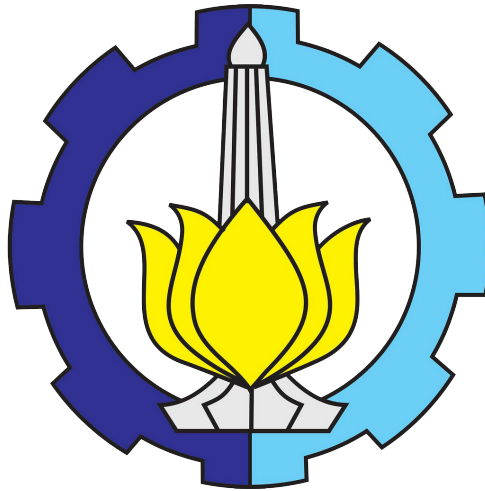


Laporan Praktikum Jaringan Komputer



Kelompok 13 :

Ariq Maulana Tazakka	5024211039
Mochammad Hilmi R.	5024211008
Reynaldo Ferdinand W.	5024211050
Wildan Jarod Tyas S.	5024211026

Fakultas Teknik Elektro dan Informatika Cerdas Departemen
Teknik Komputer

Modul 1

Wireless Connection

1 Pendahuluan

Pada Wireless Jaringan Komputer, terdapat setidaknya 3 jenis, yaitu Point-to-Point Protocol (PPP), Point-to-multipoint dan Wireless Bridging.

Point-to-Point Protocol (PPP) adalah data link protokol yang umum digunakan dalam membangun hubungan langsung antara dua node jaringan. Hal ini dapat menyediakan koneksi otentikasi, transmisi enkripsi (menggunakan ECP, RFC 1968), dan kompresi. Jenis ini biasanya digunakan untuk menghubungkan jaringan antar 2 gedung atau antar 2 BTS (Base Transceiver Station).

Point-to-multipoint adalah pendekatan yang paling populer untuk komunikasi nirkabel yang memiliki banyak node, tujuan akhir atau pengguna akhir. Jenis ini biasanya digunakan untuk membuat wifi atau hotspot yang berasal dari 1 sumber disebar ke banyak client dalam suatu jaringan.

Wireless Bridging digunakan untuk menghubungkan dua segmen LAN melalui tautan nirkabel. Kedua segmen akan berada di subnet yang sama dan terlihat seperti dua switch Ethernet yang dihubungkan oleh kabel ke semua komputer di subnet.

Untuk mengembangkan jaringan komputer berbasis wireless yang berkualitas dan mempunyai ketersediaan tinggi, penggunaan 3 jenis ini perlu disesuaikan dengan kebutuhan dan kondisi nya, sehingga kali ini saya akan membahasnya 1 persatu dari 3 jenis koneksi wireless tersebut.

2 Tujuan Praktikum

mengetahui dan memahami 3 jenis koneksi pada jaringan Wireless

3 Alat dan Bahan

Berikut adalah alat dan bahan yang digunakan untuk praktikum :

1. 2 Router Mikrotik dengan support Wireless
2. 2 Laptop
3. 2 Kabel LAN
4. Aplikasi Winbox

4 Topologi

berikut adalah topologi yang digunakan :

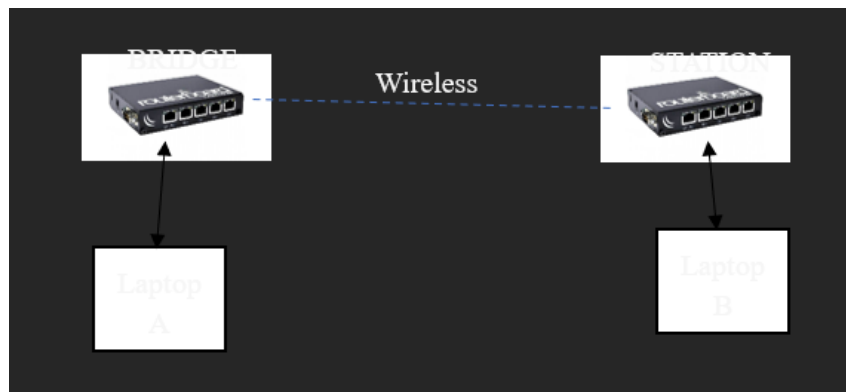


figure.1 Topologi

5 Langkah Percobaan

1. Persiapan Awal

- (a) Sambungkan PC dan Router mikrotik sesuai dengan topologi
- (b) Matikan Firewall pada Laptop
- (c) Masuk ke aplikasi Winbox
- (d) Pada bagian Neighbour, check apakah ada IP 0000 identity mikrotik
- (e) Reset mikrotik ke 0000
- (f) Lalu tekan connect

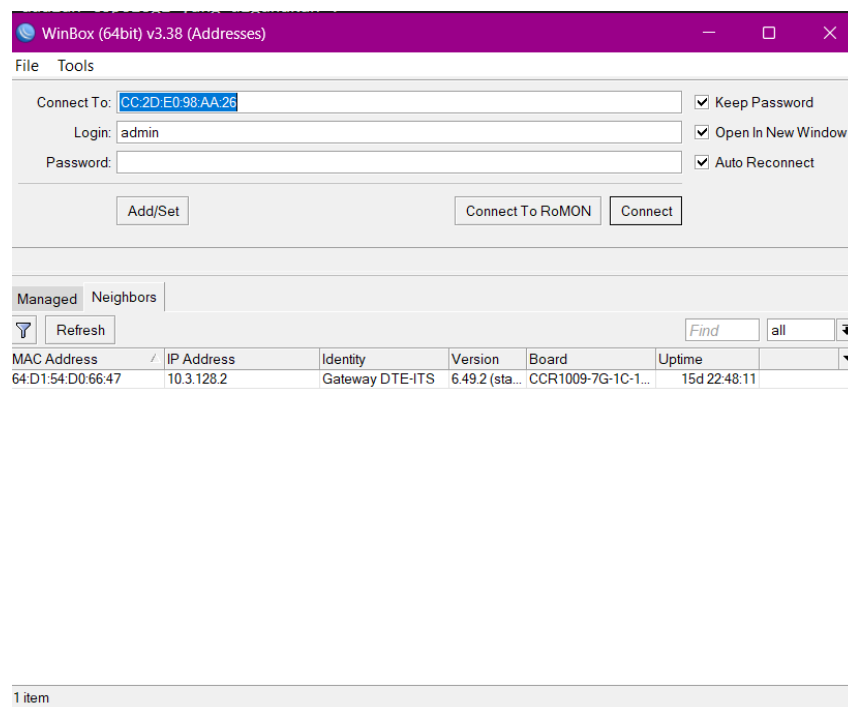


figure.2 WinBox interface

2. Wireless Point to Point

- (a) Pertama lakukan konfigurasi IP address pada masing-masing router, pilih menu IP > Address > (+) > Address : (IP Address pada router) , Interface : (interface yang tersambung) disini wlan di set sebagai network 35.35.35.0/24

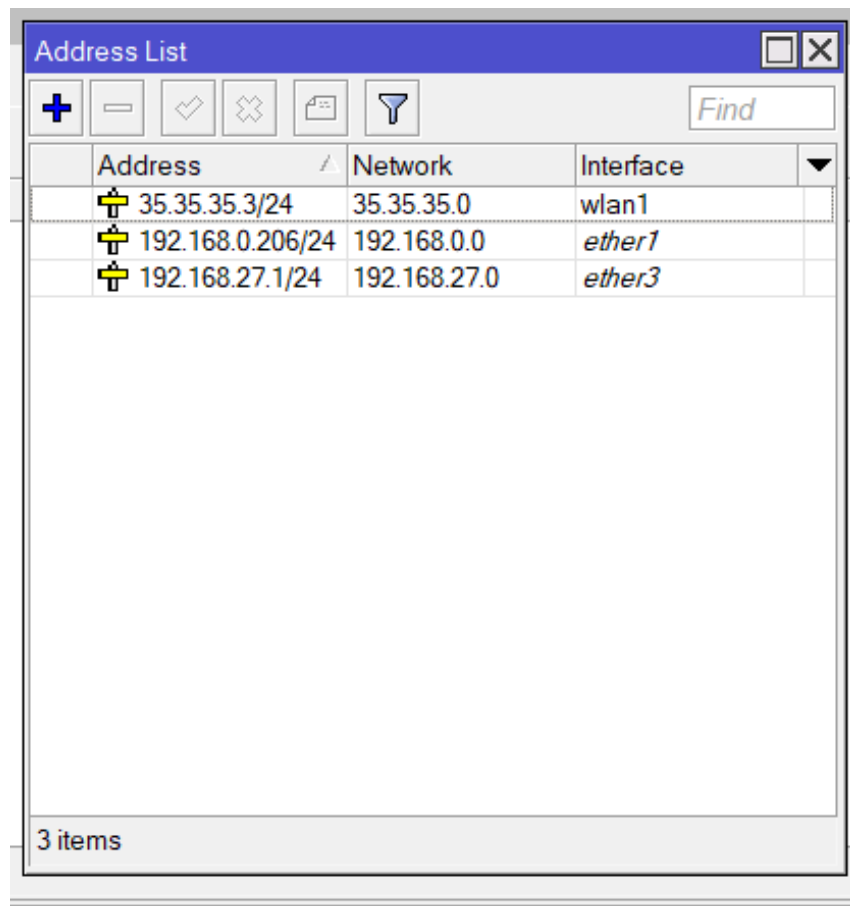


figure.3 Address Configuration

- (b) konfigurasi Router satu sebagai Bridge, pilih menu Wireless > Wlan 1 > Mode : Bridge
- (c) set SSID sesuai dengan keinginan
disini SSID diset sebagai : CobaHubungkesini

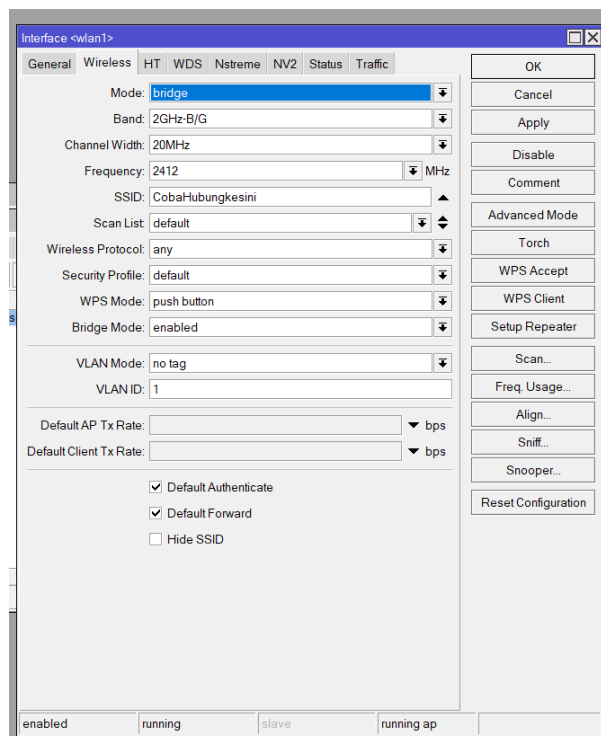


figure.4 Bridge Router Configuration

- (d) konfigurasi Router dua sebagai Station, pilih menu Wireless > Wlan 1 > Mode : Station
- (e) hubungkan dengan SSID pada router satu, di window yang sama pilih scan.. > SSID : (SSID milik router satu) > connect

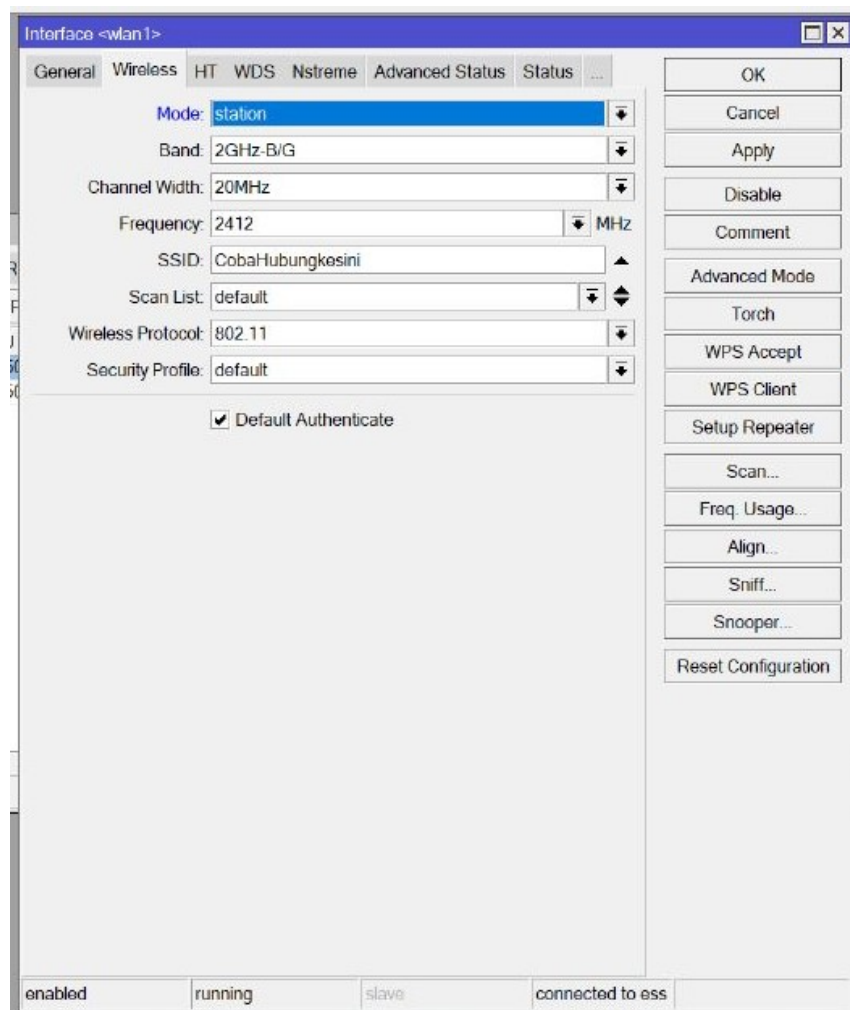


figure.5 Station Router Configuration

- (f) konfigurasi selesai, dapat dilakukan tes ping

3. Wireless Point to Multipoint

- (a) Pertama lakukan konfigurasi IP address pada masing-masing router, pilih menu IP > Address > (+) > Address : (IP Address pada router) , Interface : (interface yang tersambung) disini wlan di set sebagai network 35.35.35.0/24

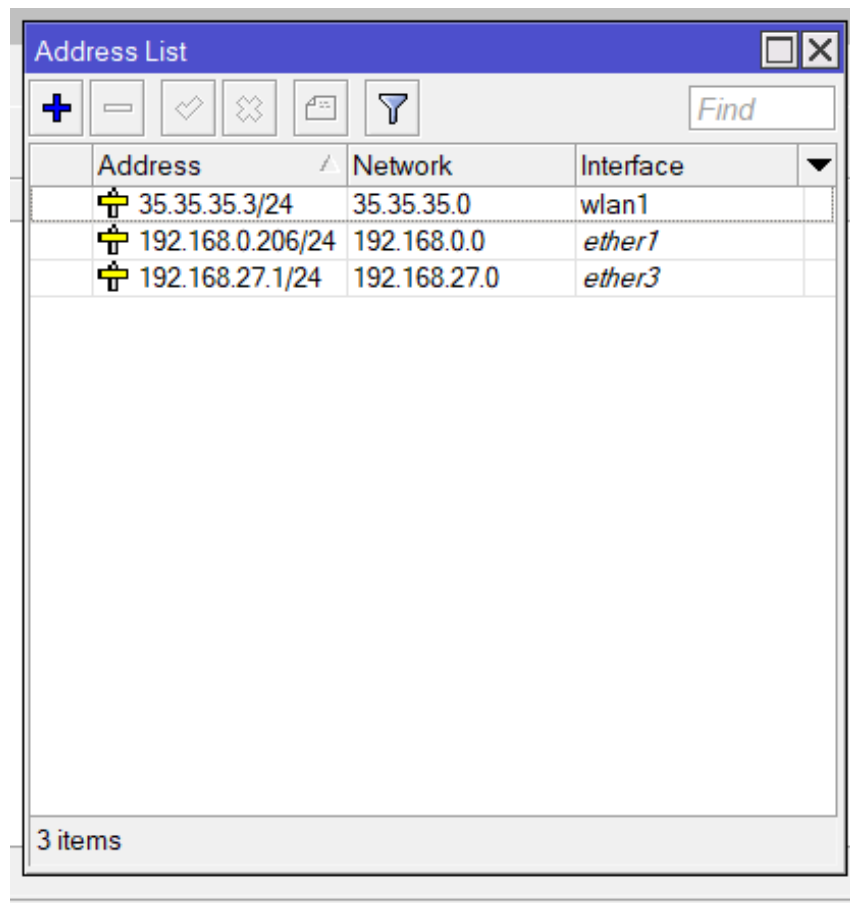


figure.6 Address Configuration

- (b) konfigurasi Router satu sebagai ApBridge, pilih menu Wireless > Wlan 1 > Mode : Ap Bridge
- (c) set SSID sesuai dengan keinginan
disini SSID diset sebagai : CobaHubungkesini

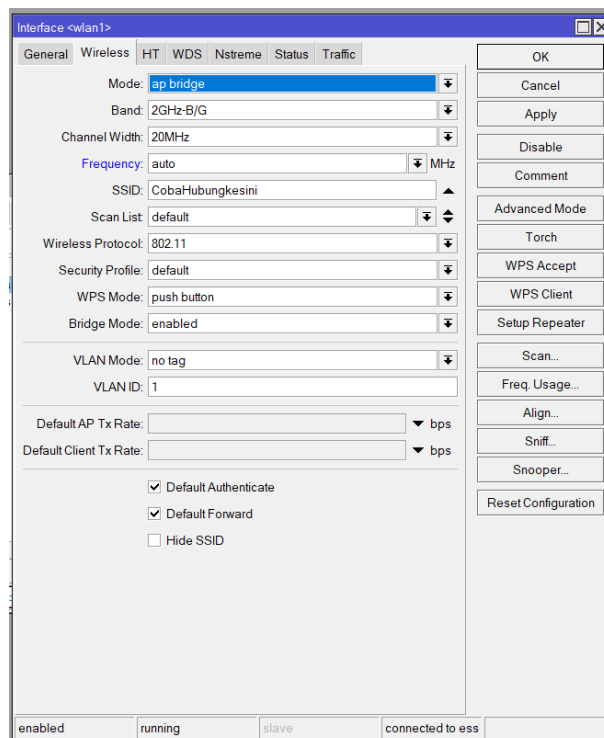


figure.7 Ap Bridge Router Configuration

- (d) konfigurasi Router dua sebagai Station, pilih menu Wireless > Wlan 1 > Mode : Station
- (e) hubungkan dengan SSID pada router satu, di window yang sama pilih scan.. > SSID : (SSID milik router satu) > connect

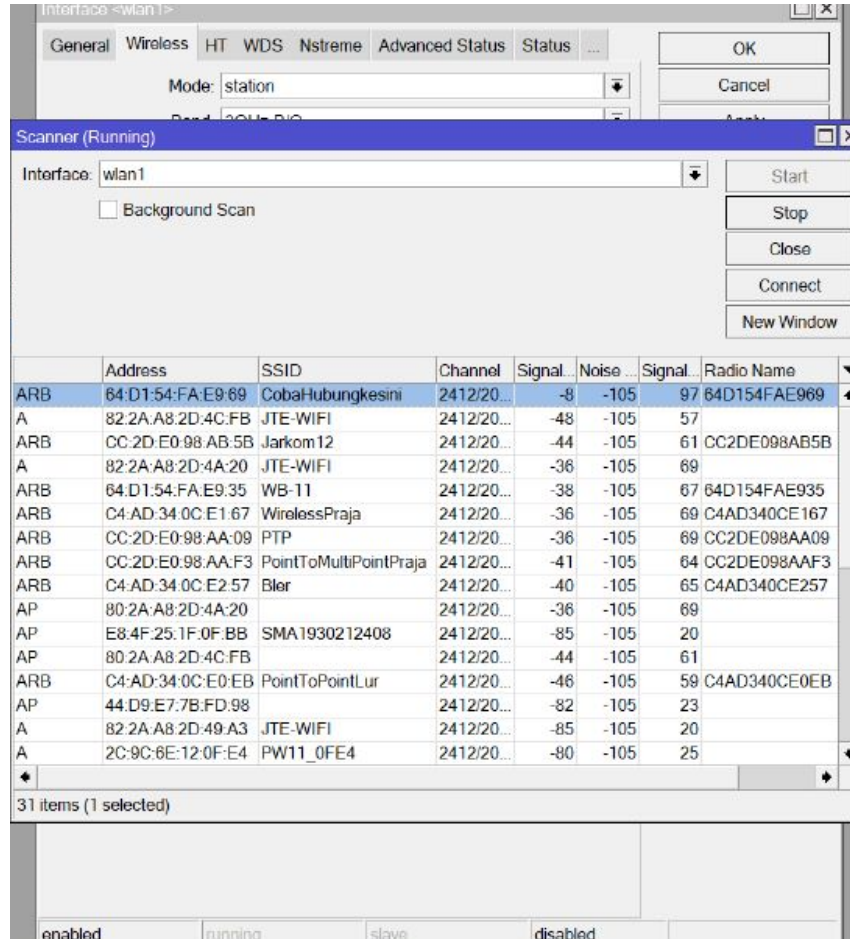


figure.8 Station Router Connect

- (f) konfigurasi selesai, dapat dilakukan tes ping

4. Wireless Bridging

- (a) Pertama lakukan konfigurasi IP address pada masing-masing router, pilih menu IP > Address > (+) > Address : (IP Address pada router) , Interface : (interface yang tersambung) disini wlan di set sebagai network 35.35.35.0/24

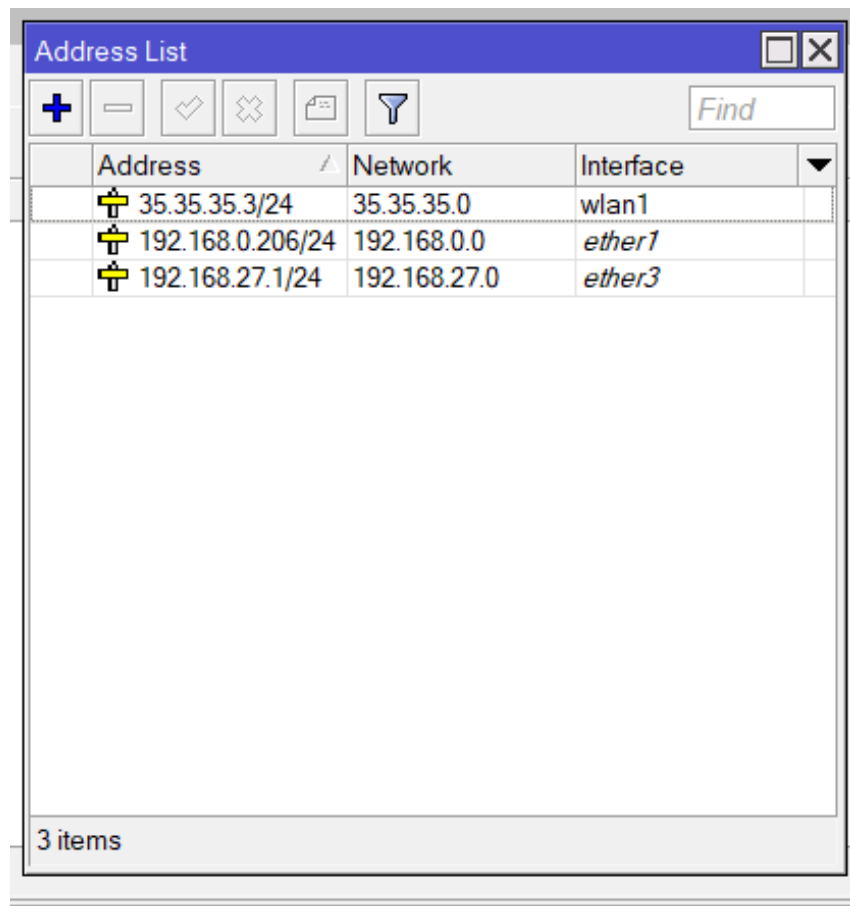


figure.9 Address Configuration

- (b) konfigurasi Router satu sebagai Bridge, pilih menu Wireless > Wlan 1 > Mode : Bridge
- (c) set SSID sesuai dengan keinginan
disini SSID diset sebagai : CobaHubungkesini

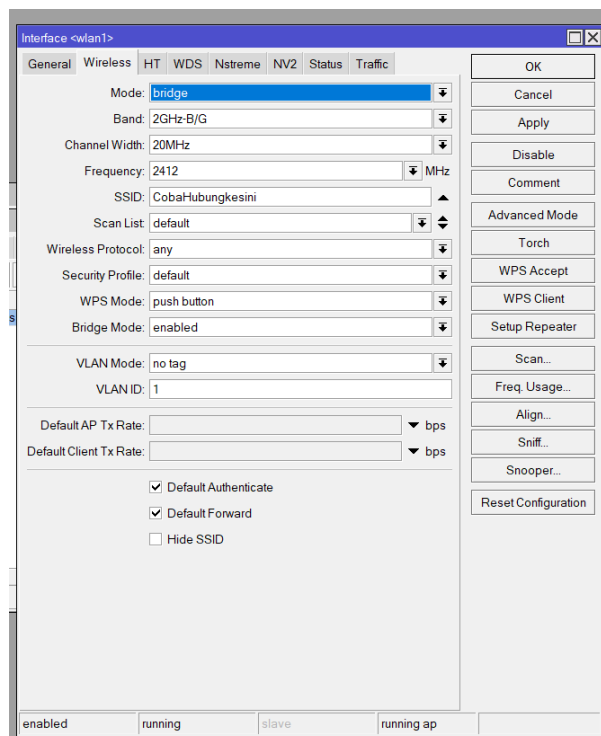


figure.10 Bridge Router Configuration

- (d) konfigurasi Router dua sebagai Station, pilih menu Wireless > Wlan 1 > Mode : Station Pseudobridge
- (e) hubungkan dengan SSID pada router satu, pada window yang sama pilih scan.. > SSID : (SSID milik router satu) > connect

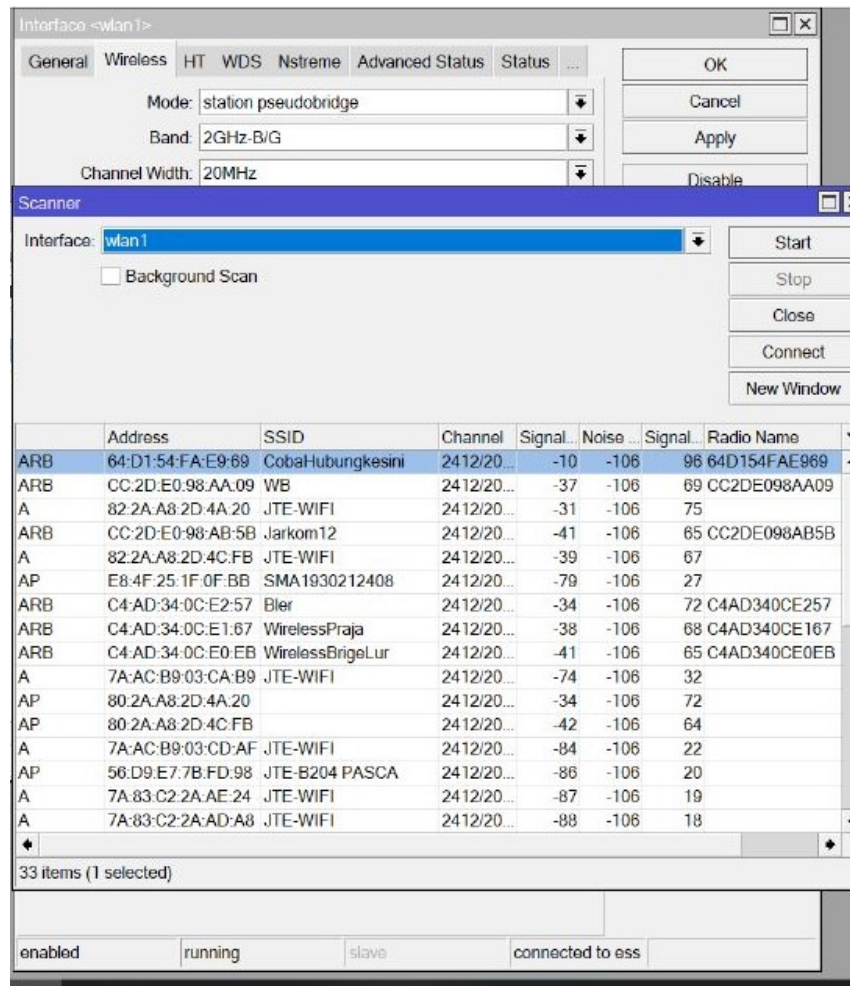


figure.11 Station Router Connect

- (f) buat bridge baru untuk untuk interface, pilih menu Bridge > (+) > nama : (sesuai keinginan)
- (g) hubungkan bridge dengan port, pada window yang sama pilih port > (+) > interface : wlan1, bridge : (brigde yang sama dengan tadi)

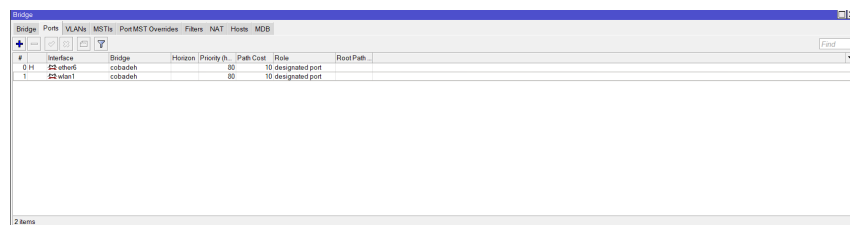


figure.12 Station Router Connect

- (h) set ip laptop agar sesuai dengan ip network yang terhubung

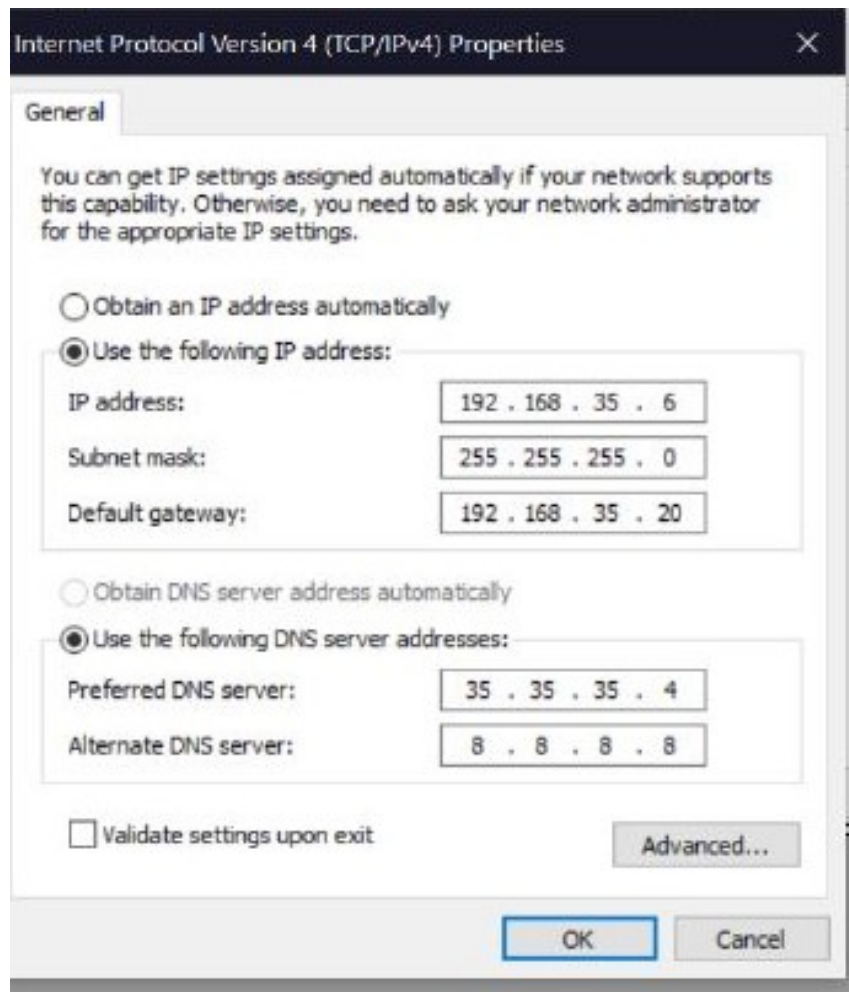


figure.13 set ip laptop

(i) konfigurasi selesai, dapat dilakukan tes ping

6 Hasil Percobaan

1. Point to Point Experiment

ping dari bridge router

```

Terminal <1>
MMM MMM KKK TTTTTTTTTT KKK
MMM MMM III KKK KKK RRRRRR OOOOOO TTT III KKK KKK
MMM MM MMM III KKKKK RRR RRR OOO OOO TTT III KKKKK
MMM MMM III KKK KKK RRRRRR OOO OOO TTT III KKK KKK
MMM MMM III KKK KKK RRR RRR OOOOOO TTT III KKK KKK

MikroTik RouterOS 6.42.1 (c) 1999-2018 http://www.mikrotik.com/

[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments

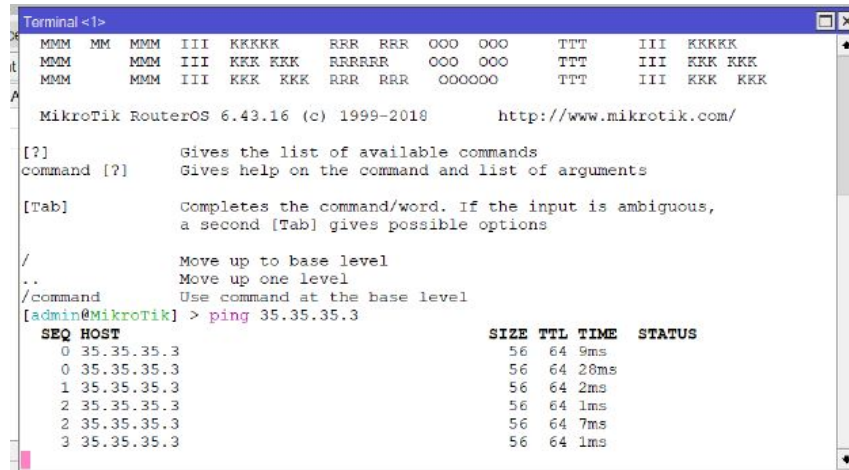
[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options

/ Move up to base level
.. Move up one level
/command Use command at the base level
[admin@MikroTik] > ping 35.35.35.4
  SEQ HOST                SIZE TTL TIME  STATUS
    0 35.35.35.4           56  64 3ms
    1 35.35.35.4           56  64 4ms
    2 35.35.35.4           56  64 0ms
    3 35.35.35.4           56  64 2ms

```

figure.14 Ping Station Router

ping dari station router



```
Terminal<1>
MMM MM MMM III KKKKK RRR RRR OOO OOO TTT III KKKKK
MMM MM MMM III KKK KKK RRRRRR OOO OOO TTT III KKK KKK
MMM MM MMM III KKK KKK RRR RRR OOOOOO TTT III KKK KKK

MikroTik RouterOS 6.43.16 (c) 1999-2018 http://www.mikrotik.com/

[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments

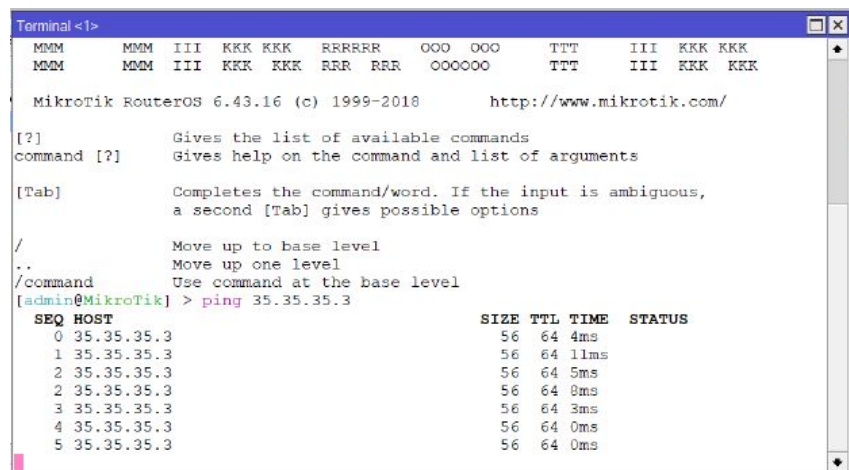
[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options

/ Move up to base level
.. Move up one level
/command Use command at the base level
[admin@MikroTik] > ping 35.35.35.3
  SEQ HOST                                SIZE TTL TIME  STATUS
  0 35.35.35.3                            56 64 9ms
  0 35.35.35.3                            56 64 28ms
  1 35.35.35.3                            56 64 2ms
  2 35.35.35.3                            56 64 1ms
  2 35.35.35.3                            56 64 7ms
  3 35.35.35.3                            56 64 1ms
```

figure.15 Ping Bridge Router

2. Point to Multipoint Experiment

tes Ping dari Station Router



```
Terminal<1>
MMM MM MMM III KKK KKK RRRRRR OOO OOO TTT III KKK KKK
MMM MM MMM III KKK KKK RRR RRR OOOOOO TTT III KKK KKK

MikroTik RouterOS 6.43.16 (c) 1999-2018 http://www.mikrotik.com/

[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments

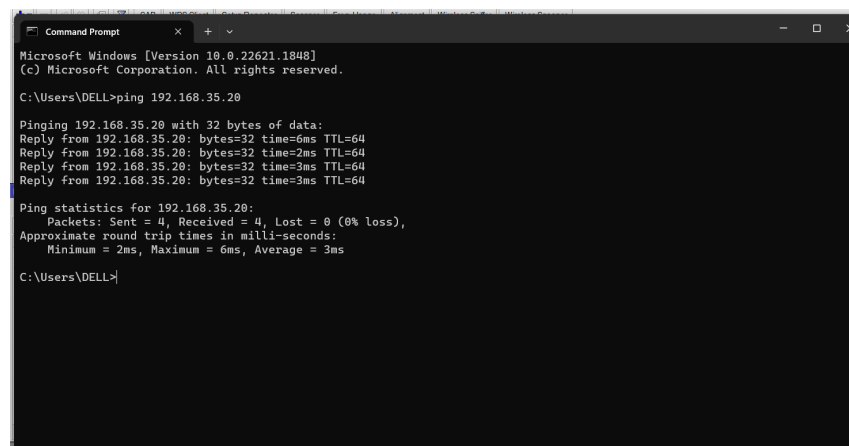
[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options

/ Move up to base level
.. Move up one level
/command Use command at the base level
[admin@MikroTik] > ping 35.35.35.3
  SEQ HOST                                SIZE TTL TIME  STATUS
  0 35.35.35.3                            56 64 4ms
  1 35.35.35.3                            56 64 11ms
  2 35.35.35.3                            56 64 5ms
  2 35.35.35.3                            56 64 8ms
  3 35.35.35.3                            56 64 3ms
  4 35.35.35.3                            56 64 0ms
  5 35.35.35.3                            56 64 0ms
```

figure.16 test Ping Station Router

3. Wireless Bridge Experiment

tes ping dari laptop



```
Command Prompt
Microsoft Windows [Version 10.0.22621.1848]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DELL>ping 192.168.35.20

Pinging 192.168.35.20 with 32 bytes of data:
Reply from 192.168.35.20: bytes=32 time=6ms TTL=64
Reply from 192.168.35.20: bytes=32 time=2ms TTL=64
Reply from 192.168.35.20: bytes=32 time=3ms TTL=64
Reply from 192.168.35.20: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.35.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 6ms, Average = 3ms

C:\Users\DELL>
```

figure.17 test Ping Laptop

7 Kesimpulan

Jaringan Komputer berbasis Wireless dapat menggunakan Teknologi Point to Point, Point to Multipoint dan Wireless Bridging

Modul 2

Wireless Connection

1 Pendahuluan

Pada modul ini, kita akan membahas konfigurasi routing static dan routing dinamis pada perangkat MikroTik. Routing merupakan proses pengiriman data antara dua atau lebih jaringan yang berbeda.

Dalam modul ini, kita akan membahas konsep dasar routing, macam-macam routing statis dan dinamis, serta langkah-langkah untuk mengkonfigurasi kedua jenis routing ini pada perangkat MikroTik.

Sebelum memulai pembahasan routing, penting untuk memahami konsep dasar jaringan dan subnetting. Jaringan terdiri dari sejumlah perangkat yang terhubung satu sama lain, seperti komputer, printer, dan perangkat jaringan lainnya. Setiap perangkat dalam jaringan memiliki alamat IP yang unik.

Subnetting adalah proses pembagian jaringan menjadi subnet yang lebih kecil. Dengan subnetting, kita dapat mengoptimalkan penggunaan alamat IP dan membagi jaringan menjadi beberapa segmen yang terpisah.

Dalam routing, terdapat yang namanya protokol routing. Protokol routing adalah aturan yang digunakan oleh perangkat jaringan untuk memilih jalur terbaik bagi pengiriman data antara jaringan yang berbeda. Ada dua jenis protokol routing utama: routing static dan routing dinamis.

2 Tujuan Praktikum

Mengetahui dan memahami konfigurasi routing static dan routing dinamis pada Mikrotik.

3 Alat dan Bahan

Berikut adalah alat dan abhan yang digunakan:

1. 2 perangkat router mikrotik.
2. Aplikasi Winbox.
3. 3 kabel LAN

4 Topologi

berikut adalah topologi yang digunakan :

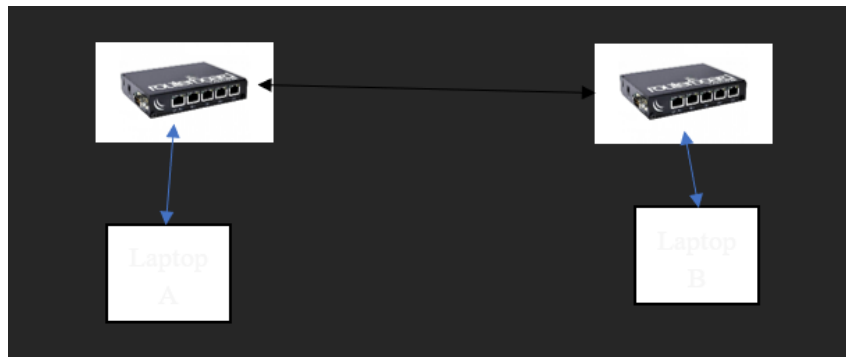


figure.1 Topologi

5 Langkah Percobaan

1. Persiapan Awal

- Sambungkan PC dan Router mikrotik sesuai dengan topologi
- Matikan Firewall pada Laptop
- Masuk ke aplikasi Winbox
- Pada bagian Neighbour, check apakah ada IP 0000 identity mikrotik
- Reset mikrotik ke 0000
- Lalu tekan connect

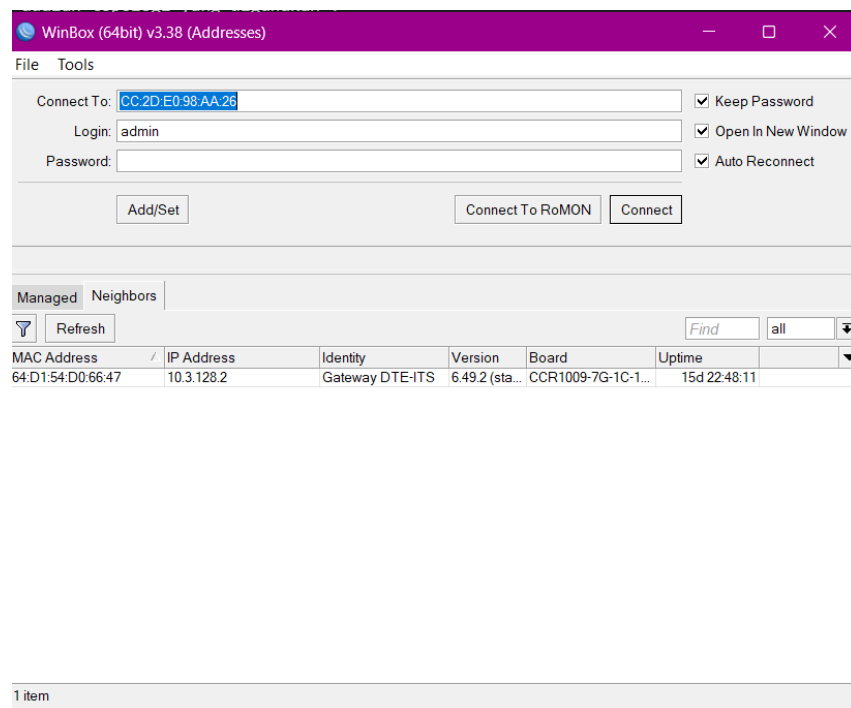


figure.2 WinBox interface

2. Static Routing

- Pertama lakukan konfigurasi IP address pada masing-masing router, pilih menu IP > Address > (+) > Address : (IP Address pada router) , Interface : (interface yang tersambung)

- (b) Untuk melakukan routing statis, pilih menu IP > Routes > (+) > Dst . Address : (IP network client router lawan) , Gateway : (IP yang menghubungkan kedua router)
- (c) Apabila sudah benar, maka akan terlihat tulisan 'reachable'

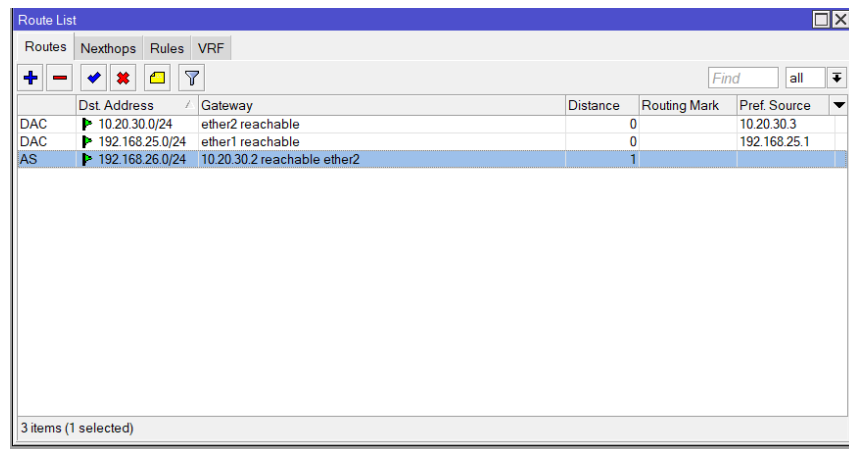


figure.3 Route list

- (d) Setelah itu konfigurasi DHCP servernya untuk klien yang akan terhubung, pilih menu IP > DHCP Server > (+) > DHCP Server Interface : (interface yang menghubungkan pada laptop)

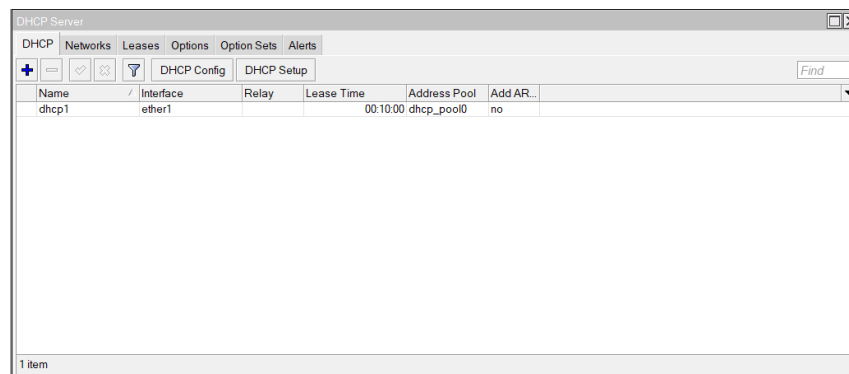


figure.4 DHCP Server setup

- (e) Static routing selesai, dapat dilakukan test ping

3. Dynamic Routing

- (a) Untuk melakukan routing dinamis, pilih menu Routing > RIP > Interface > (+) > Interface : (interface yang menghubungkan antar router) > Apply > OK
- (b) Kemudian masih dalam window RIP, pilih tab Networks > (+) > Address : (masukan semua IP Network yang terhubung dengan router) > OK
- (c) Masih dalam window RIP, pilih tab Neighbour > (+) > Address : (alamat IP router lawan)

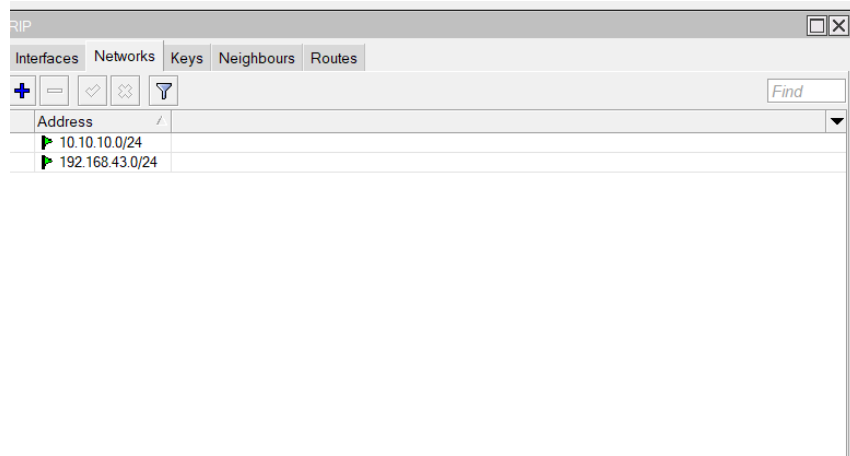


figure.5 Dynamic RIP table

- (d) Setelah itu lakukan konfigurasi IP pada masing-masing laptop agar sesuai dengan yang sudah terisi pada winbox
- (e) Dynamic routing selesai, dapat dilakukan test ping

6 Hasil Percobaan

1. Static Routing

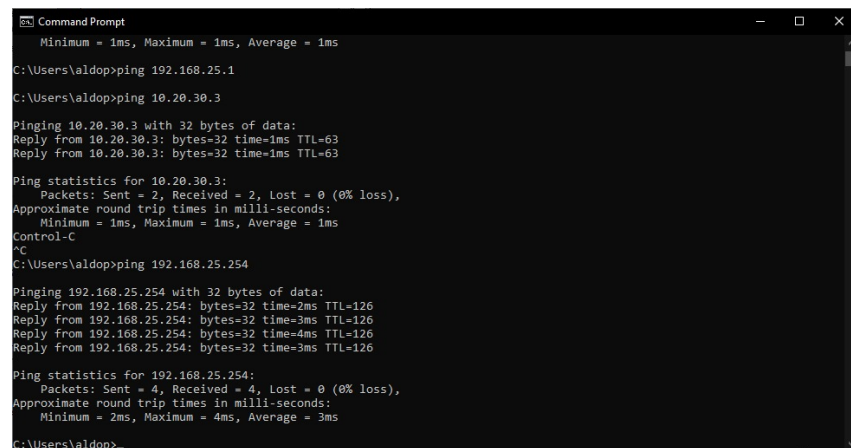


figure.6 Static Routing Testing

2. Dynamic Routing


```
Terminal <1>
SEQ HOST                                SIZE TTL TIME  STATUS
0 192.168.43.2                          56 127 lms
1 192.168.43.2                          timeout
2 192.168.43.2                          timeout
3                                         no route to host
4                                         no route to host
5                                         no route to host
6                                         no route to host
7                                         no route to host
8                                         no route to host
sent=9 received=1 packet-loss=88% min-rtt=lms avg-rtt=lms max-rtt=lms

[admin@MikroTik] > ping 192.168.43.2
SEQ HOST                                SIZE TTL TIME  STATUS
0 192.168.43.2                          56 127 lms
1 192.168.43.2                          56 127 lms
2 192.168.43.2                          56 127 lms
3 192.168.43.2                          56 127 lms
4 192.168.43.2                          56 127 lms
5 192.168.43.2                          56 127 lms
6 192.168.43.2                          56 127 lms
sent=7 received=7 packet-loss=0% min-rtt=lms avg-rtt=lms max-rtt=lms

[admin@MikroTik] >
```

figure.7 Dynamic Routing Testing

7 Kesimpulan

Static dan Dynamic Routing dapat menghubungkan komputer melalui kabel LAN

Modul 3

Mengelola dan Membagi Bandwidth dengan Menggunakan QoS(Simple Queue)

1 Pendahuluan

Dalam lingkungan jaringan yang padat, sering kali beberapa pengguna menggunakan aplikasi atau protokol yang mengkonsumsi bandwidth yang tinggi, seperti video streaming atau file sharing, sementara pengguna lainnya mungkin hanya perlu menggunakan aplikasi yang membutuhkan bandwidth yang lebih rendah, seperti browsing web atau email. Tanpa manajemen bandwidth yang efektif, pengguna dengan aplikasi berat bisa mendominasi sebagian besar bandwidth, menyebabkan kualitas layanan yang buruk bagi pengguna lain.

2 Tujuan Praktikum

Mengetahui cara melimitasi dan memanagemen bandwidth untuk suatu jaringan dengan banyak pengguna.

3 Alat dan Bahan

Berikut adalah Alat dan Bahan untuk praktikum:

1. 1 RouterOS Mikrotik
2. 2 Laptop
3. Kabel LAN
4. Software WinBox

4 Topologi

berikut adalah topologi yang digunakan :

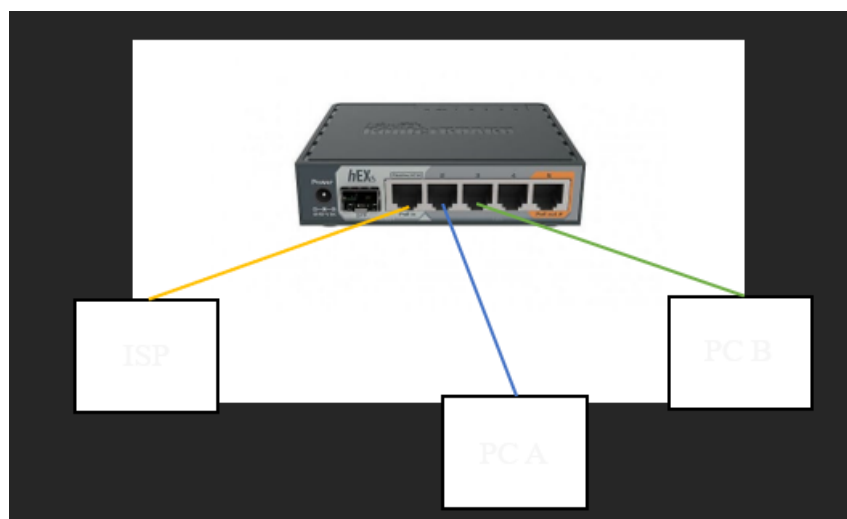


figure.1 Topologi

5 Langkah Percobaan

1. Sambungkan PC dan router mikrotik sesuai dengan topologi
2. Matikan firewall di laptop
3. Masuk ke aplikasi Winbox
4. Pada bagian Neighbour, check apakah ada IP 0000 identity mikrotik
5. Reset mikrotik ke 0000
6. Lalu tekan connect

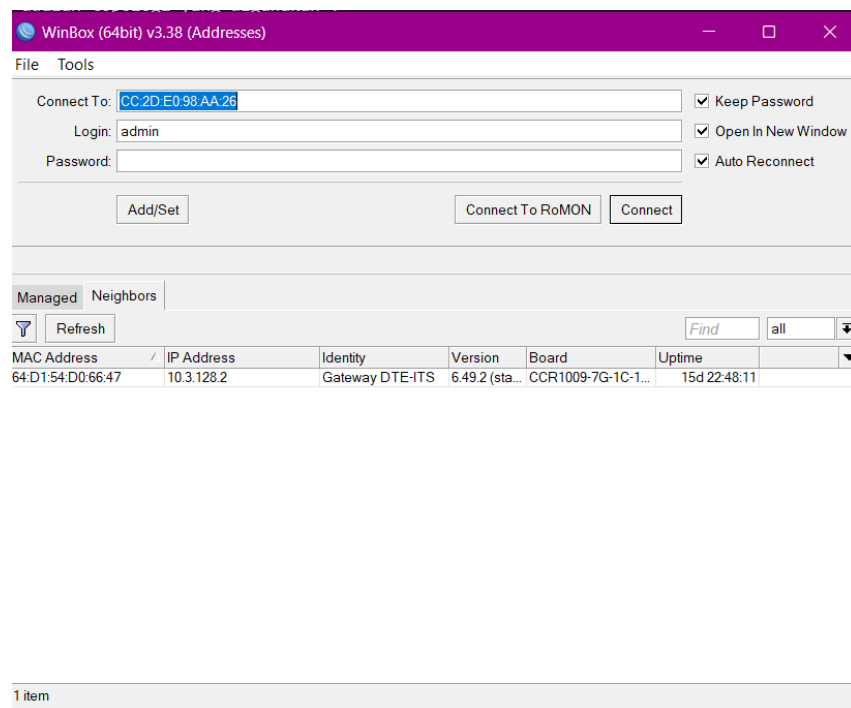


figure.2 WinBox interface

7. Lakukan konfigurasi DHCP agar dapat terhubung dengan ISP, pilih menu IP > DHCP Client > (+) > Interface : ether 1 (yang terhubung pada ISP)
8. Kemudian secara otomatis akan didapatkan IP dari ISP
9. Lalu pilih menu IP > Firewall > NAT > Chain : srcnat, Out. Interface : ether 1
10. Kemudian pilih menu IP > Firewall > NAT > Action : masquerade
11. Setelah itu atur routes untuk ether 1 secara static, pilih menu IP > Routes > (+) > Dst Address : 0.0.0.0/0, Gateway : (gateway IP address yang telah diberikan ISP) > Apply
12. Setelah terlihat status “reachable” pada Route List, kemudian atur DNS
13. Untuk melakukan limitasi bandwidth sederhana, pilih New Simple Queue > General
14. Pada kolom Target Address, masukkan IP address yang akan diberikan limitasi
15. Dan pada kolom Max Limit, masukkan besar maximum limitasi yang akan diberikan

6 Hasil Percobaan

7 Kesimpulan

Pembatasan bandwidth suatu jaringan dapat dilakukan dengan menggunakan QoS(Simple Queue)

8 Tugas modul

1. Manfaat dari implementasi QoS dalam manajemen bandwidth yaitu dapat memberikan prioritas layanan, pengendalian trafik, mengurangi latency, meningkatkan kinerja aplikasi, dan mengoptimalkan penggunaan sumber daya.
2. Situasi dimana prioritas bandwidth menjadi kritis yaitu dalam jaringan yang digunakan oleh beberapa penyewa atau pelanggan. QoS menjadi penting untuk memastikan pengalaman yang adil dan memenuhi kebutuhan masing-masing penyewa. Tanpa QoS, satu penyewa yang menggunakan sebagian besar bandwidth dapat mengorbankan kinerja dan kualitas layanan untuk penyewa lainnya. Dengan menerapkan QoS, prioritas bandwidth dapat diberikan berdasarkan kebutuhan dan kesepakatan kontrak dengan setiap penyewa, sehingga memastikan distribusi yang adil dan memenuhi persyaratan layanan.
3. Risiko atau masalah yang mungkin muncul saat mengimplementasikan QoS salah satunya yaitu Konfigurasi QoS dapat menjadi kompleks, terutama dalam jaringan yang kompleks atau besar. Mengidentifikasi aplikasi atau layanan yang memerlukan prioritas bandwidth tertentu, mengatur aturan prioritas, dan mengelola kebijakan QoS dapat melibatkan pengaturan yang rumit. Kesalahan konfigurasi dapat mengakibatkan gangguan jaringan atau distribusi bandwidth yang tidak diinginkan.
4. Perbedaan antara menggunakan QoS dengan Simple Queue dan menggunakan pembatasan bandwidth biasa, seperti limitasi bandwidth pada router, terletak pada tingkat kontrol, kemampuan prioritas, dan fleksibilitas dalam mengelola lalu lintas jaringan.
5. Keunggulan menggunakan QoS (Quality of Service) dalam manajemen bandwidth dibandingkan dengan pembatasan bandwidth biasa antara lain dapat memberikan prioritas dan penyesuaian yang lebih baik, fleksibilitas dalam manajemen, dan juga pengaturan yang lebih spesifik.

Modul 4

Konfigurasi VPN(Virtual Private Network) PPTP pada Mikrotik

1 Pendahuluan

VPN atau Jaringan Pribadi Virtual (Virtual Private Network) membuat koneksi jaringan privat di antara beberapa perangkat melalui internet. VPN digunakan untuk mentransmisikan data secara aman dan anonim melalui jaringan publik. VPN bekerja dengan cara menyembunyikan alamat IP pengguna dan mengenkripsi data sehingga tidak dapat dibaca oleh siapa pun yang tidak berwenang untuk menerimanya.

Salah satu service yang biasa digunakan untuk membangun sebuah jaringan VPN adalah Point to Point Tunnel Protocol (PPTP). Sebuah koneksi PPTP terdiri dari Server dan Client. Mikrotik RouterOS bisa difungsikan baik sebagai server maupun client atau bahkan diaktifkan keduanya bersama dalam satu mesin yang sama. Feature ini sudah termasuk dalam package PPP sehingga anda perlu cek di menu system package apakah paket tersebut sudah ada di router atau belum. Fungsi PPTP Client juga sudah ada di hampir semua OS, sehingga kita bisa menggunakan Laptop/PC sebagai PPTP Client.

Biasanya PPTP ini digunakan untuk jaringan yang sudah melewati multihop router (Routed Network). Jika anda ingin menggunakan PPTP pastikan di Router anda tidak ada rule yang melakukan blocking terhadap protocol TCP 1723 dan IP Protocol 47/GRE karena service PPTP menggunakan protocol tersebut.

2 Tujuan Praktikum

Mengetahui cara menggunakan dan mengkonfigurasi VPN PPTP pada router mikrotik.

3 Alat dan Bahan

Berikut adalah Alat dan Bahan untuk praktikum:

1. 2 Cloud Core Router
2. 3 Kabel UTP (LAN)
3. 3 Laptop
4. Software Winbox

4 Topologi

berikut adalah topologi yang digunakan :

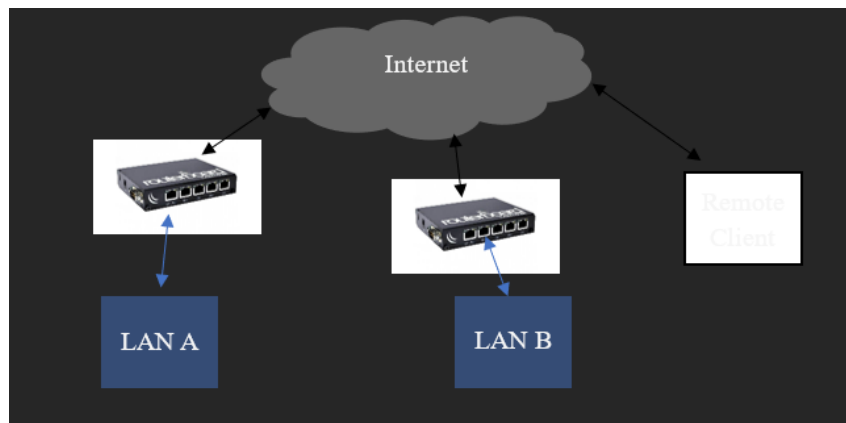


figure.1 Topologi

5 Langkah Percobaan

1. Sambungkan PC dan router mikrotik sesuai dengan topologi
2. Matikan firewall di laptop
3. Masuk ke aplikasi Winbox
4. Pada bagian Neighbour, check apakah ada IP 0000 identity mikrotik
5. Reset mikrotik ke 0000
6. Lalu tekan connect

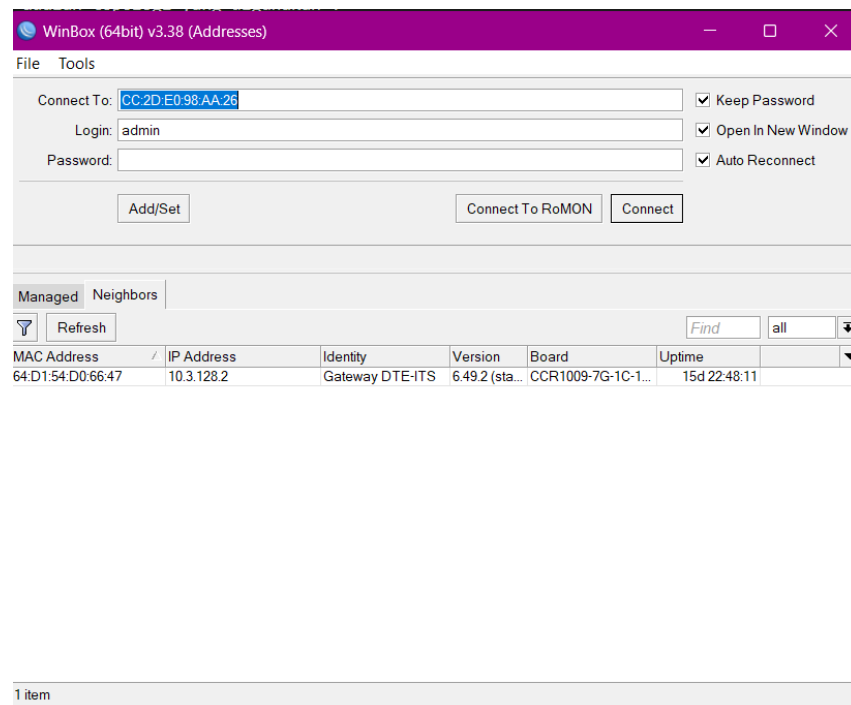


figure.2 WinBox interface

7. Lakukan konfigurasi DHCP agar dapat terhubung dengan ISP, pilih menu IP > DHCP Client > (+) > Interface : ether 1 (yang terhubung pada ISP)
8. Kemudian secara otomatis akan didapatkan IP dari ISP

9. Lalu pilih menu IP > Firewall > NAT > Chain : srcnat, Out. Interface : ether 1
10. Kemudian pilih menu IP > Firewall > NAT > Action : masquerade
11. Setelah itu atur routes untuk ether 1 secara static, pilih menu IP > Routes > (+) > Dst Address : 0.0.0.0/0, Gateway : (gateway IP address yang telah diberikan ISP) > Apply
12. Setelah terlihat status “reachable” pada Route List, kemudian atur DNS
13. Untuk mengaktifkan PPTP server, pilih menu PPP > Interface > PPTP Server > Default Profile : default encryption
14. Kemudian buatlah secret untuk mengakses server, pilih menu New PPP Secret > Profile : default encryption , Local Address : (address PPTP server) , Remote Address : (IP yang akan diberikan ke client)

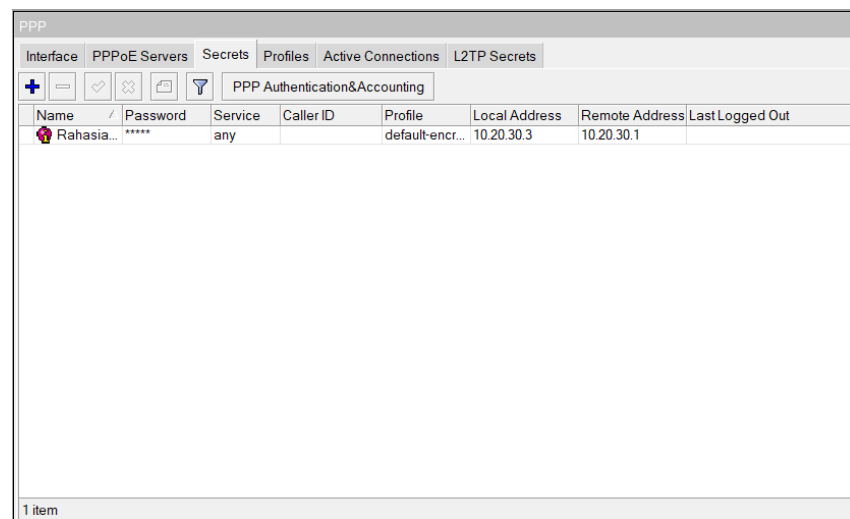


figure.3 PPP Server

15. Isikan nama dan password, pastikan nama dan password mudah untuk diingat
16. Lalu lakukan konfigurasi client PPTP, pilih menu PPTP Client > New Interface > Connect To : (IP public server yang dituju)
17. Kemudian pada kolom User dan Password, masukkan nama dan password sesuai secret yang sudah dibuat
18. Setelah itu lakukan static routing, pilih menu New Route > Dst. Address : (jaringan local router lawan) , Gateway : (IP PPTP tunnel pada router lawan)

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
S	0.0.0.0/0	192.168.35.1 reachable ether1	1		
DAS	0.0.0.0/0	10.3.145.1 reachable ether2	1		
DAC	10.3.145.0/24	ether2 reachable	0		10.3.145.159
DAC	10.20.30.1	<pptp-Rahasia hilmi> reachable, pptp-out1 reachable	0		10.20.30.3
S	192.168.30.0/24	10.20.30.3 unreachable	1		
AS	192.168.30.0/24	10.20.30.1 reachable pptp-out1	1		
DAC	192.168.35.0/24	ether1 reachable	0		192.168.35.1

7 items

figure.4 Virtual Route List

19. Untuk melakukan remote client, perlu dibuat secret baru dengan cara yang sama dengan sebelumnya
20. Agar remote client dapat terhubung ke server, perlu dilakukan setup connection pada sisi client
21. Pergi ke setting dan pilih menu Network and Sharing Center > Set up new connection or network > Connect to a workplace > Use My Internet Connection (VPN) > Internet address : (IP public server yang dituju) > Next
22. Kemudian masukkan nama dan password sesuai secret yang sudah dibuat untuk remote client

Settings

Edit VPN connection

Server name or address
10.3.145.159

VPN type
Automatic

Type of sign-in info
User name and password

User name (optional)
Rahasia global

Password (optional)
.....

Save Cancel

figure.5 VPN Set up

6 Hasil Percobaan

Router Test


```

Terminal <1>
168 192.168.30.1 56 64 0ms
169 192.168.30.1 56 64 0ms
170 192.168.30.1 56 64 0ms
171 192.168.30.1 56 64 0ms
172 192.168.30.1 56 64 0ms
173 192.168.30.1 56 64 0ms
174 192.168.30.1 56 64 0ms
175 192.168.30.1 56 64 0ms
176 192.168.30.1 56 64 0ms
177 192.168.30.1 56 64 0ms
178 192.168.30.1 56 64 0ms
179 192.168.30.1 56 64 0ms
sent=180 received=180 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
SEQ HOST SIZE TTL TIME STATUS
180 192.168.30.1 56 64 0ms
181 192.168.30.1 56 64 0ms
182 192.168.30.1 56 64 0ms
183 192.168.30.1 56 64 0ms
184 192.168.30.1 56 64 0ms
185 192.168.30.1 56 64 0ms
186 192.168.30.1 56 64 0ms
187 192.168.30.1 56 64 0ms
188 192.168.30.1 56 64 0ms

```

figure.6 Route Testing

Client test

```

Command Prompt
Microsoft Windows [Version 10.0.19045.3086]
(c) Microsoft Corporation. All rights reserved.

C:\Users\asus>ping 192.168.35.1

Pinging 192.168.35.1 with 32 bytes of data:
Reply from 192.168.35.1: bytes=32 time=3ms TTL=64
Reply from 192.168.35.1: bytes=32 time=4ms TTL=64
Reply from 192.168.35.1: bytes=32 time=4ms TTL=64
Reply from 192.168.35.1: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.35.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 4ms, Average = 3ms

C:\Users\asus>

```

figure.7 Client Testing

7 Kesimpulan

PPTP dapat digunakan untuk membuat suatu Virtual Private Network(VPN)

8 Tugas modul

1. PPTP memiliki kelemahan yaitu tidak menyediakan mekanisme otentikasi server yang kuat, sehingga rentan terhadap serangan MITM(Man in the Middle). Untuk memitigasi hal ini dapat dilakukan dengan menambahkan enkripsi tambahan, misalnya dengan menggunakan protokol enkripsi seperti L2TP/IPSec untuk melindungi lalu lintas data yang dikirim melalui koneksi PPTP.
2. Alternatif protokol VPN yang lebih aman dibandingkan PPTP salah satunya adalah IPSec(Internet Protocol Security). Apabila dibandingkan dengan PPTP, IPSec menggunakan enkripsi yang lebih kuat, protokol otentikasi yang lebih andal, dan sering kali memiliki mekanisme keamanan tambahan yang diperbarui secara teratur.
3. Kelebihan utama yang dimiliki oleh PPTP yaitu kemudahan implementasi. Penggunaan dan pengaturan PPTP lebih sederhana dibandingkan dengan protokol VPN

lain yang mungkin memerlukan konfigurasi yang lebih kompleks. Selain itu PPTP juga memiliki kinerja yang cepat karena protokol PPTP dirancang untuk memberikan koneksi yang stabil dan responsive dengan beban yang lebih rendah pada jaringan.

4. Beberapa kekurangan dan batasan penggunaan PPTP sebagai protokol VPN antara lain yaitu kelemahan keamanan, tidak didukung oleh banyak perangkat, tidak dapat melewati firewall yang ketat, dan tidak dapat digunakan di beberapa negara atau jaringan.
5. Langkah-langkah untuk mendiagnosis masalah dalam mengkonfigurasi VPN PPTP diantaranya yaitu dengan memeriksa pengaturan server VPN, memeriksa pengaturan klien VPN, memeriksa koneksi jaringan, memeriksa firewall dan perangkat jaringan, memeriksa log dan pesan kesalahan, mencoba koneksi dari lokasi lain, atau dengan memperbarui perangkat lunak.
6. Solusi alternatif PPTP diantaranya yaitu dengan menggunakan protokol VPN berbasis SSL(Secure Socket Layer)/TLS(Transport Layer Security) maupun VPN berbasis SSH(Secure Shell). Dan apabila masalah masih tidak dapat diatasi, pertimbangkan menggunakan layanan VPN yang tersedia secara komersial.

Modul 5

Implementasi dan Konfigurasi IP Version 6

1 Pendahuluan

Semakin berkembangnya teknologi, maka semakin banyak alokasi alamat jaringan yang diperlukan. Maka dari itu dikembangkanlah Internet Protocol Address v6 (IPv6). Internet Protocol Address v6 (IPv6) adalah standar protokol yang digunakan untuk mengidentifikasi dan mengarahkan alamat jaringan dalam jaringan komputer. Dibandingkan dengan pendahulunya, IPv4, IPv6 memiliki format alamat yang lebih panjang dengan 128 bit, yang memungkinkan jumlah alamat yang jauh lebih besar, sehingga dapat mengatasi kekurangan alamat IPv4 yang semakin berkurang. IPv6 juga mendukung fitur-fitur tambahan, termasuk pemantauan aliran lalu lintas, keamanan yang ditingkatkan, dan kualitas layanan yang lebih baik, menjadikannya solusi jangka panjang untuk pertumbuhan Internet yang pesat dan kebutuhan alamat yang terus berkembang.

2 Tujuan Praktikum

1. Mengetahui bagaimana konfigurasi static routing menggunakan IPV6
2. Mengimplementasikan konfigurasi IPV6 pada perangkat mikrotik

3 Alat dan Bahan

berikut adalah alat dan bahan yang digunakan:

1. 2 Router
2. 3 Kabel LAN
3. 2 Laptop
4. Koneksi Internet

4 Topologi

berikut adalah topologi yang digunakan :

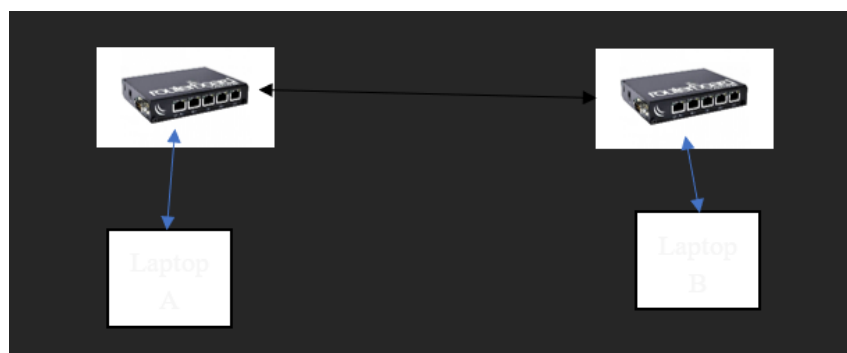


figure.1 Topologi

5 Langkah Percobaan

1. Persiapan Awal

- (a) Sambungkan PC dan router mikrotik sesuai dengan topologi
- (b) Matikan firewall di laptop
- (c) Masuk ke aplikasi Winbox
- (d) Pada bagian Neighbour, check apakah ada IP 0000 identity mikrotik
- (e) Reset mikrotik ke 0000
- (f) Lalu tekan connect

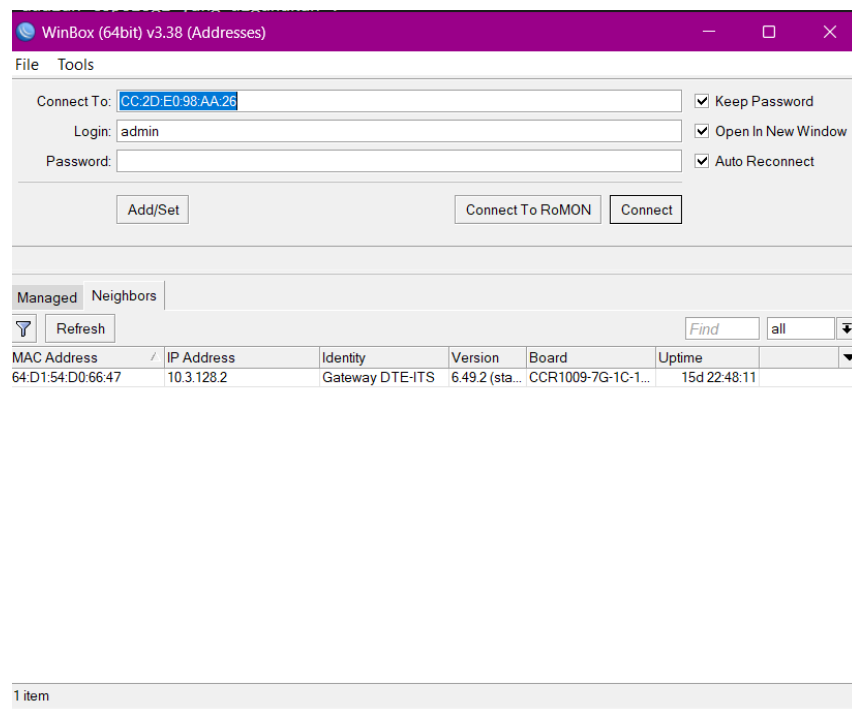


figure.2 WinBox interface

- (g) Aktifkan IPv6 pada kedua router, pilih menu System > Packages > ipv6 [Enable]
- (h) Kemudian reboot router, melalui System > Reboot
- (i) Pada bagian Neighbour, check apakah ada IP Address versi 6
- (j) Lalu tekan connect
- (k) Lakukan konfigurasi DHCP agar dapat terhubung dengan ISP, pilih menu IP > DHCP Client > (+) > Interface : ether 1 (yang terhubung pada ISP)
- (l) Kemudian secara otomatis akan didapatkan IP dari ISP

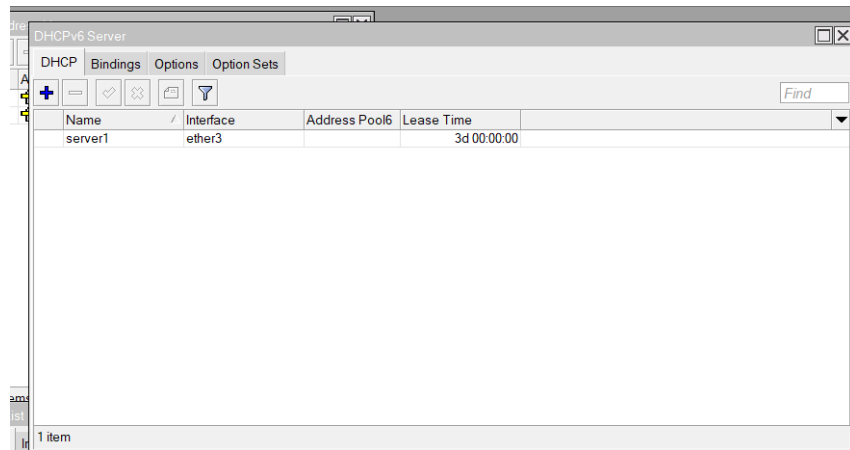


figure.3 DHCP Client

2. Static v6 Routing

- (a) Konfigurasi IPv6 pada kedua router, pilih menu IPv6 > Addresses > (+) > Address : (IP address versi 6 pada router) , Interface : (Interface yang tersambung ke laptop) , Advertise [Check]

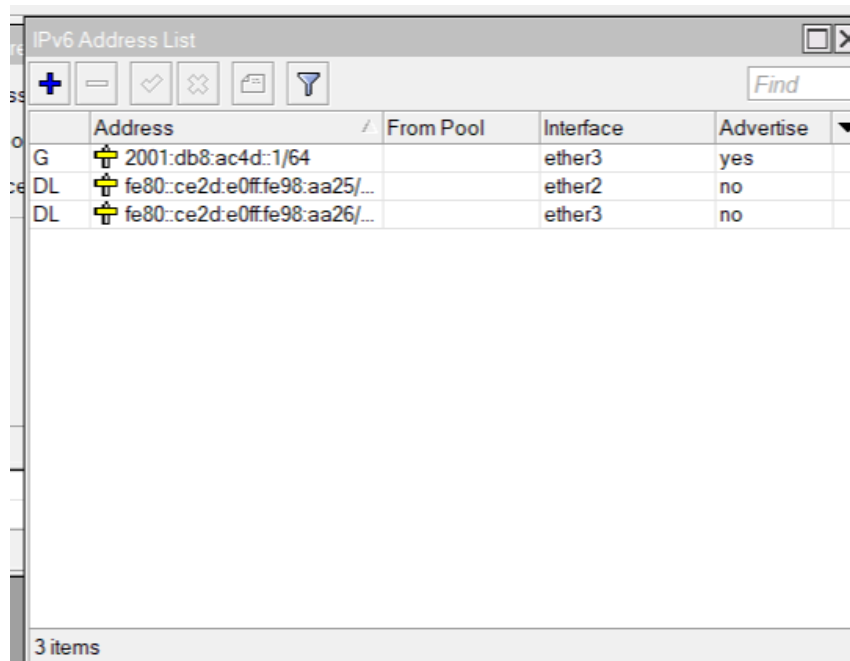


figure.4 Address List

- (b) Selanjutnya lakukan static routing pada masing-masing router (sama seperti melakukan routing IP versi 4), pilih menu IPv6 > Routes > (+) > Dst. Address : (IP versi 6 jaringan lawan) , Gateway : (gunakan link local IP address yang menghubungkan antara kedua router)

	Dst Address	Gateway	Distance
AS	2001:db8:3c4d::/64	fe80::ce2d:e0ff:fe98:aadb%ether2 reachable	1
DAC	2001:db8:ac4d::/64	ether3 reachable	0
XS	2019:db8:20::/64	2019:db8:100:2	1

3 items

figure.5 Static v6 Routing

- (c) Setelah itu uji koneksi antara kedua jaringan dengan melakukan test ping dari router (sama seperti melakukan test ping pada IP versi 4)

3. Dynamic v6 Routing

- (a) Konfigurasi IPv6 pada kedua router, pilih menu IPv6 > Addresses > (+) > Address : (IP address versi 6 pada router) , Interface : (Interface yang tersambung ke laptop) , Advertise [Check]

	Address	From Pool	Interface	Advertise
G	2001:db8:ac4d::1/64		ether3	yes
DL	fe80::ce2d:e0ff:fe98:aa25/...		ether2	no
DL	fe80::ce2d:e0ff:fe98:aa26/...		ether3	no

3 items

figure.6 Address List

- (b) selanjutnya lakukan Dynamic Routing dengan pilih menu Route > RIPng > (+) > interface : (interface yang dipakai)

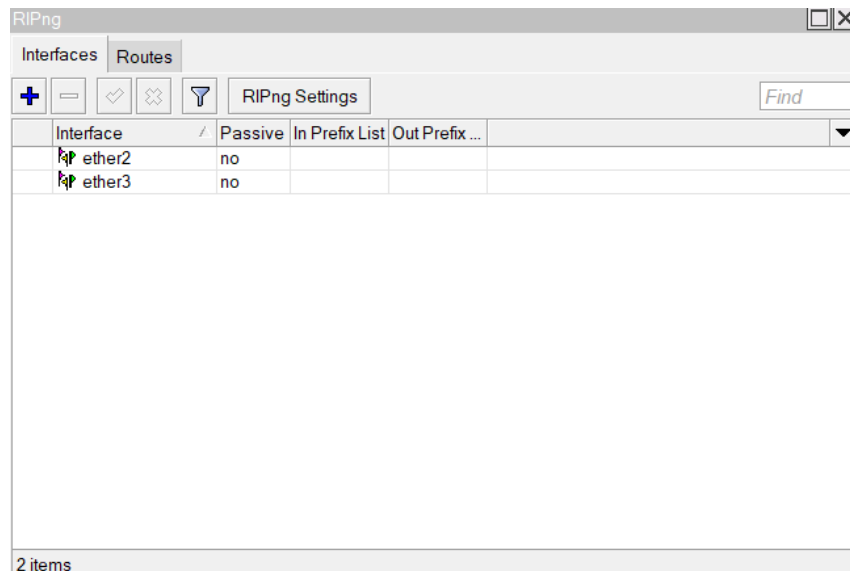


figure.7 RiPng Dynamic v6 Routing

(c) bila sudah dilakukan dengan benar, maka di routing akan muncul route baru

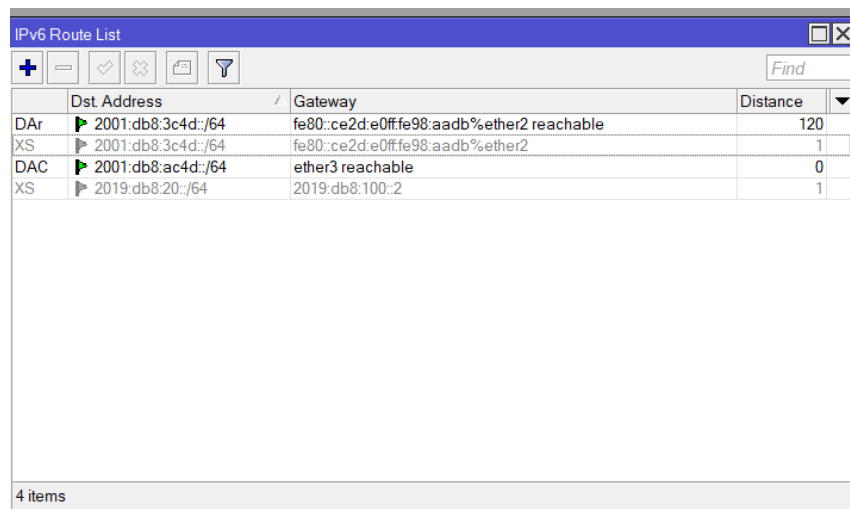


figure.8 Dynamic v6 Route

6 Hasil Percobaan

1. Static v6 Routing

```

Terminal <1>
14 2001:db8:3c4d::1          56 64 0ms echo reply
15 2001:db8:3c4d::1          56 64 0ms echo reply
16 2001:db8:3c4d::1          56 64 0ms echo reply
17 2001:db8:3c4d::1          56 64 0ms echo reply
18 2001:db8:3c4d::1          56 64 0ms echo reply
19 2001:db8:3c4d::1          56 64 0ms echo reply
sent=20 received=20 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
SEQ HOST                      SIZE TTL TIME STATUS
20 2001:db8:3c4d::1          56 64 0ms echo reply
21 2001:db8:3c4d::1          56 64 0ms echo reply
22 2001:db8:3c4d::1          56 64 0ms echo reply
23 2001:db8:3c4d::1          56 64 0ms echo reply
24 2001:db8:3c4d::1          56 64 0ms echo reply
25 2001:db8:3c4d::1          56 64 0ms echo reply
26 2001:db8:3c4d::1          56 64 0ms echo reply
27 2001:db8:3c4d::1          56 64 0ms echo reply
28 2001:db8:3c4d::1          56 64 0ms echo reply
29 2001:db8:3c4d::1          56 64 0ms echo reply
30 2001:db8:3c4d::1          56 64 0ms echo reply
31 2001:db8:3c4d::1          56 64 0ms echo reply
32 2001:db8:3c4d::1          56 64 0ms echo reply
sent=33 received=33 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
[admin@MikroTik] >

```

figure.9 Static v6 Testing

2. Dynamic v6 Routing

```

Terminal <1>
0 2001:db8:3c4d::1          56 64 0ms echo reply
1 2001:db8:3c4d::1          56 64 0ms echo reply
2 2001:db8:3c4d::1          56 64 0ms echo reply
3 2001:db8:3c4d::1          56 64 0ms echo reply
4 2001:db8:3c4d::1          56 64 0ms echo reply
5 2001:db8:3c4d::1          56 64 0ms echo reply
6 2001:db8:3c4d::1          56 64 0ms echo reply
7 2001:db8:3c4d::1          56 64 0ms echo reply
8 2001:db8:3c4d::1          56 64 0ms echo reply
9 2001:db8:3c4d::1          56 64 0ms echo reply
10 2001:db8:3c4d::1          56 64 0ms echo reply
11 2001:db8:3c4d::1          56 64 0ms echo reply
12 2001:db8:3c4d::1          56 64 0ms echo reply
13 2001:db8:3c4d::1          56 64 0ms echo reply
14 2001:db8:3c4d::1          56 64 0ms echo reply
15 2001:db8:3c4d::1          56 64 0ms echo reply
16 2001:db8:3c4d::1          56 64 0ms echo reply
17 2001:db8:3c4d::1          56 64 0ms echo reply
18 2001:db8:3c4d::1          56 64 0ms echo reply
19 2001:db8:3c4d::1          56 64 0ms echo reply
sent=20 received=20 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
SEQ HOST                      SIZE TTL TIME STATUS
20 2001:db8:3c4d::1          56 64 0ms echo reply

```

figure.10 Dynamic v6 Testing

7 Kesimpulan

IPv6 merupakan teknologi baru pengembangan dari IPv4 yang digunakan untuk meningkatkan layanan jaringan internet

8 Tugas modul

1. Faktor yang mempengaruhi kinerja koneksi IPv6 antara dua jaringan antara lain:
 - (a) Kualitas dan keandalan perangkat atau infrastruktur jaringan seperti router, switch, dan firewall dapat mempengaruhi kecepatan dan stabilitas koneksi IPv6.
 - (b) Ketersediaan bandwidth menjadi faktor penting dalam menentukan kinerja koneksi IPv6. Jika bandwidth terbatas, kinerja koneksi IPv6 dapat terpengaruhi dan menyebabkan penurunan kecepatan tranfer data.

- (c) Latensi yang tinggi dapat mempengaruhi kinerja koneksi IPv6 dengan menyebabkan penundaan dalam pengiriman data. Beberapa faktor yang dapat menyebabkan latensi tinggi meliputi jarak fisik antara dua jaringan, kualitas jalur jaringan, dan waktu pemrosesan di perangkat jaringan.
 - (d) Faktor lain yang dapat mempengaruhi kinerja koneksi IPv6 adalah konfigurasi dan pemeliharaan jaringan yang kurang tepat. Kesalahan konfigurasi, kegagalan pemeliharaan rutin, atau kekurangan pembaruan perangkat lunak jaringan dapat mengakibatkan masalah kinerja.
 - (e) Implementasi kualitas layanan (Quality of Service/QoS).
2. Untuk menambahkan dua subnet tambahan dengan ukuran /64 dari jaringan IPv6 2001:0db8:1234::/48, dapat dilakukan dengan langkah-langkah berikut:
- (a) Tentukan batas subnet yang diinginkan, karena /64 adalah ukuran default untuk subnet dalam IPv6, maka dapat digunakan dua /64 subnet berurutan dari blok 2001:0db8:1234::/48.
 - (b) Hitung alamat subnet baru, pertahankan 48 bit pertama dari alamat jaringan 2001:0db8:1234::/48 dan tentukan 16 bit terakhir untuk setiap subnet baru. Ambil 16 bit terakhir dari alamat jaringan, yaitu ::/64 sebagai subnet pertama (alamat subnet pertama 2001:0db8:1234::/64). Tambahkan 1 pada 16 bit terakhir dari alamat subnet pertama, yaitu ::1/64 sebagai subnet kedua (alamat subnet kedua 2001:0db8:1234::1/64).
 - (c) Setelah menghitung alamat subnet baru, konfigurasi perangkat jaringan yang relevan untuk mengakomodasi subnet tambahan.
 - (d) Konfigurasi perangkat klien dengan alamat IPv6 yang tepat dari subnet yang sesuai bila diperlukan.

Untuk mengkonfigurasi antarmuka jaringan host, dapat dilakukan dengan metode Dynamic Host Configuration Protocol version 6 (DHCPv6) dengan langkah berikut:

- (a) Pastikan server DHCPv6 terhubung ke subnet baru dan terkonfigurasi dengan benar.
 - (b) Aktifkan protokol DHCPv6 pada host yang bersangkutan.
 - (c) Host akan mengirim permintaan alamat IPv6 ke server DHCPv6 dan menerima alamat yang ditugaskan
3. Migrasi dari IPv4 ke IPv6 diperlukan dalam jaringan saat ini karena beberapa alasan, salah satunya yaitu ketersediaan alamat IPv4 yang semakin menipis. IPv4 menggunakan format alamat 32 bit yang membatasi jumlah alamat yang tersedia, sedangkan IPv6 menggunakan format alamat 128 bit yang dapat memberikan keuntungan kapasitas alamat yang jauh lebih besar dan dapat memenuhi kebutuhan konektivitas di masa depan. Selama proses migrasi, jaringan perlu mendukung koeksistensi IPv4 dan IPv6 untuk memastikan konektivitas yang lancar bagi perangkat yang belum mendukung IPv6. Perlu dipastikan perangkat jaringan dapat melakukan translasi protokol (IPv6-IPv4) dan penyediaan tunnel (IPv6-over-IPv4) jika dibutuhkan. Migrasi ke IPv6 membutuhkan perhatian khusus terhadap keamanan jaringan. Perubahan dalam protokol, alamat, dan konfigurasi jaringan dapat mempengaruhi postur keamanan. Penting untuk memastikan bahwa infrastruktur IPv6 terlindungi dengan baik melalui penerapan kebijakan keamanan yang

sesuai dan pemantauan lalu lintas jaringan untuk mengidentifikasi dan merespons ancaman keamanan IPv6.