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 :

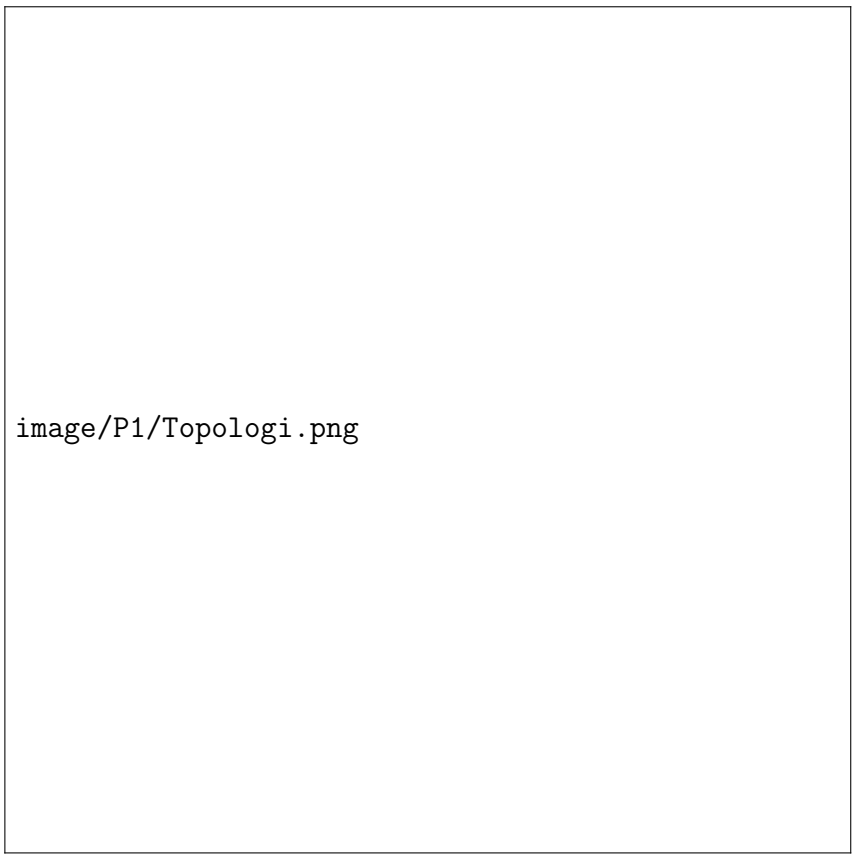

figure.1 Topologi

5 Langkah Percobaan

1.

6 Hasil Percobaan

7 Kesimpulan

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

3 Alat dan Bahan

4 Topologi

berikut adalah topologi yang digunakan :

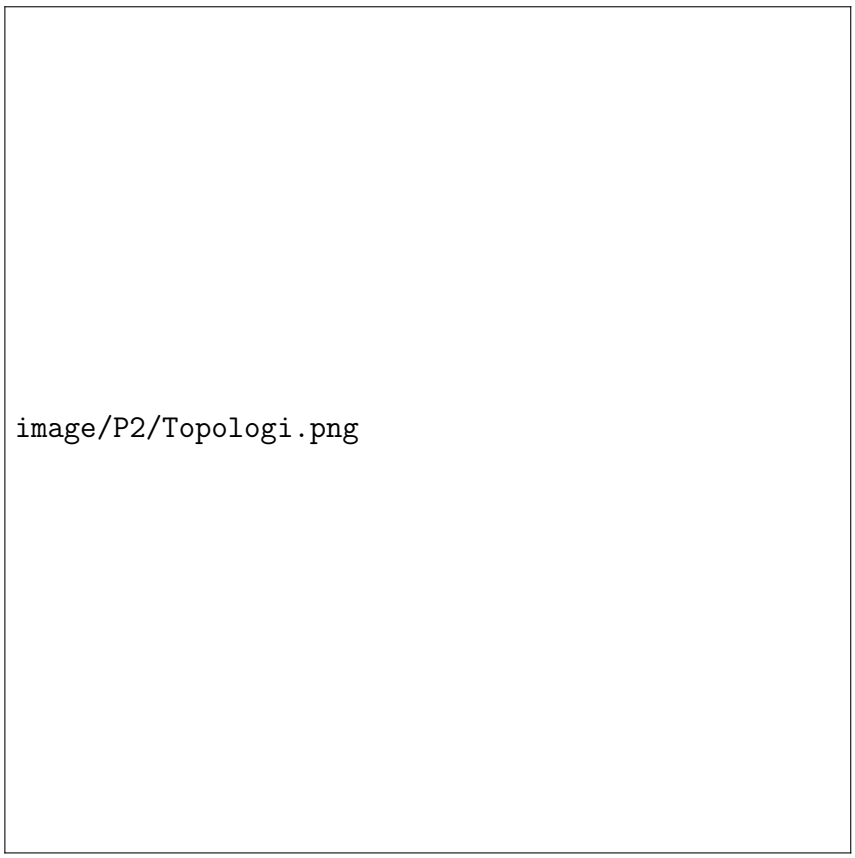

figure.1 Topologi

5 Langkah Percobaan

1.

6 Hasil Percobaan

7 Kesimpulan

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 :

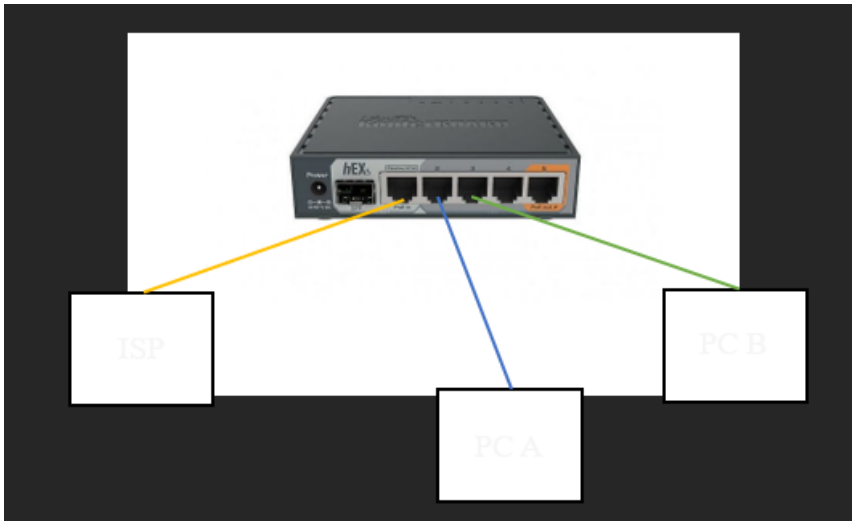

figure.1 Topologi

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
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 berdas
arkan 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, fleksiilitas dalam manajemen, dan juga pengaturan yang lebih spesifik.

Modul 4
Konfigurasi VPN(Virtual Private Network) PPTP pada Mikrotik

1 pendahuluan

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 :

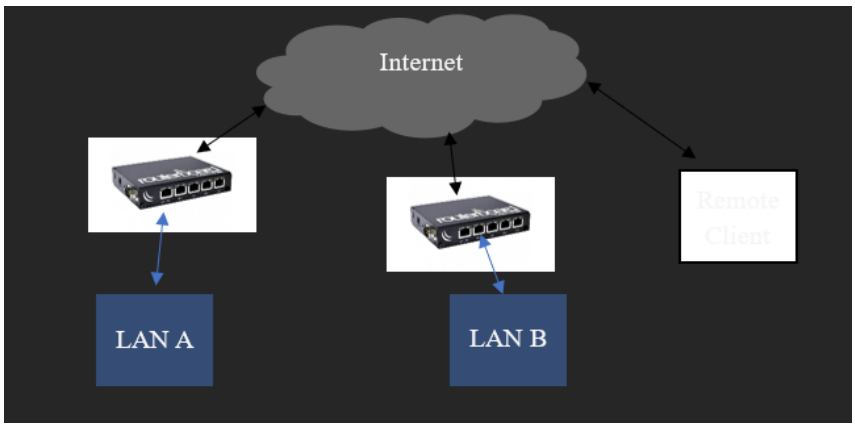

figure.1 Topologi

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
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)
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)
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

6 Hasil Percobaan

7 Kesimpulan

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 menambahakan enkripsi tambahan, misalnya dengan menggunakan protokol enkripsi seperti L2TP/IPS-
   ec 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 :

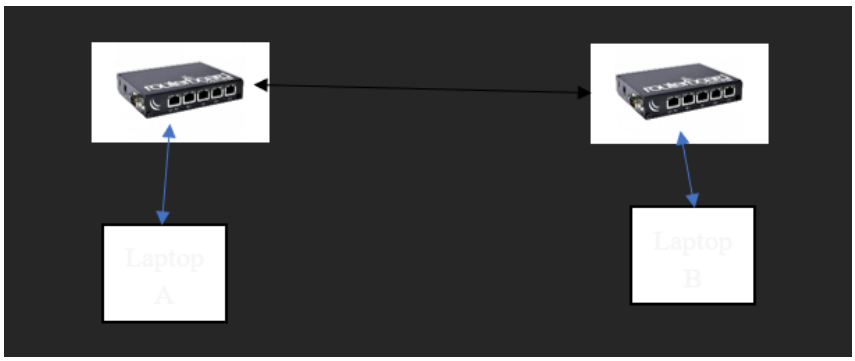

figure.1 Topologi

5 Langkah Percobaan

1.

6 Hasil Percobaan

7 Kesimpulan

8 Tugas modul