

**IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN) SERVER
MENGUNAKAN MIKROTIK UNTUK REMOTE ACCESS
DI SMK ISLAM MANBAUL HIKMAH LUWUNGRAGI**

SKRIPSI



Oleh :

NIM	: 55201190031
NAMA	: ARI IRKHAM FAUZI
JENJANG STUDI	: STRATA SATU (S1)
PROGRAM STUDI	: TEKNIK INFORMATIKA

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHADI SETIABUDI BREBES
2021**

**IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN) SERVER
MENGUNAKAN MIKROTIK UNTUK REMOTE ACCESS
DI SMK ISLAM MANBAUL HIKMAH LUWUNGRAGI**

SKRIPSI

**DIAJUKAN SEBAGAI SALAH SATU SYARAT UNTUK MENCAPAI GELAR
SARJANA PROGRAM STUDI TEKNIK INFORMATIKA**



Oleh :

NIM	: 55201190031
NAMA	: ARI IRKHAM FAUZI
JENJANG STUDI	: STRATA SATU (S1)
PROGRAM STUDI	: TEKNIK INFORMATIKA

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHADI SETIABUDI BREBES
2021**

TANDA PERSETUJUAN SEMINAR SKRIPSI

NIM : 55201190031
Nama : Ari Irkham Fauzi
Jenjang Studi : Strata Satu (S1)
Program Studi : Teknik Informatika
Judul Proposal : Implementasi Virtual Private Server (VPN) Server
Menggunakan Mikrotik Untuk Remote Access di
SMK Islam Manbaul Hikmah Luwungragi

Brebes, Maret 2021

Menyetujui,

Pembimbing I,

Agyztia Premana, S.Kom, M.Kom

Tanggal 1/9/2021

Pembimbing II,

Abdul Khamid, ST, MT

Tanggal 1/9/2021

Mengetahui,
Ka. Prodi Teknik Informatika



Agyztia Premana, S.Kom, M.Kom

Tanggal 1/9/2021

TANDA PERSETUJUAN SIDANG SKRIPSI

NIM : 55201190031
Nama : Ari Irkham Fauzi
Jenjang Studi : Strata Satu (S1)
Program Studi : Teknik Informatika
Judul Proposal : Implementasi Virtual Private Server (VPN) Server
Menggunakan Mikrotik Untuk Remote Access di
SMK Islam Manbaul Hikmah Luwunragi

Brebes, Agustus 2021

Pembimbing I,

Menyetujui,



Agyztia Premana, S.Kom., M.Kom
NIDN. 060311901

Tanggal ... 1/8/2021 ...

Pembimbing II,



Abdul Khamid, ST., MT
NIDN. 0615077203

Tanggal ... 1/8/2021 ...



Mengetahui
Ka. Prodi Teknik Informatika

Agyztia Premana, S.Kom, M.Kom
NIDN. 060311901

Tanggal ... 1/8/2021 ...

TANDA PENGESAHAN SKRIPSI

NIM : 55201190031
 Nama : Ari Irkham Fauzi
 Jenjang Studi : Strata Satu (S1)
 Program Studi : Teknik Informatika
 Judul Skripsi : Implementasi Virtual Private Network (VPN) Server
 Menggunakan Mikrotik Untuk Remote Access di SMK
 Islam Manbaul Hikmah Luwungragi

Dipertahankan di depan Tim Penguji Skripsi
 Program Studi Teknik Informatika
 Fakultas Teknik Universitas Muhadi Setiabudi Brebes Pada Tanggal
01/05/2021

Dewan Penguji

NO.	NAMA	TANDA TANGAN
1.	Agyztia Premana, S.Kom., M.Kom	
2.	Abdul Khamid, ST., MT	
3.	Nur Ariesanto Ramdhan, S.Kom., M.Kom	
4.	R.M. Herdian Bhakti, ST., MT	



Mengetahui,
 Kaprodi Teknik Informatika
Agyztia Premana, S.Kom., M.Kom
 NIDN. 060311901

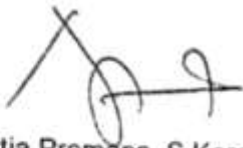
**IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN)
SERVER MENGGUNAKAN MIKROTIK UNTUK REMOTE
ACCESS
DI SMK ISLAM MANBAUL HIKMAH LUWUNGRAGI**

SKRIPSI

NIM : 55201190031
NAMA : ARI IRKHAM FAUZI

Disetujui Oleh :

Pembimbing I



Agyztia Premana, S.Kom., M.Kom
NIDN. 060311901

Pembimbing II



Abdul Khamid, ST., MT
NIDN. 0615077203



Mengetahui,
Ka. Prodi Teknik Informatika

Agyztia Premana, S.Kom., M.Kom
NIDN. 060311901

PERNYATAAN

Saya yang bertanda tangan dibawah ini :

NIM : 55201190031
Nama : Ari Irkham Fauzi
Tempat/Tgl Lahir : Brebes, 6 Agustus 1996
Alamat : Jalan Sumber Pangan No.35 Keboledan Brebes

Menyatakan bahwa dalam skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana komputer di suatu perguruan tinggi, dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Brebes, 17 Agustus 2021



Ari Irkham Fauzi

KATA PENGANTAR

Berkat rahmat Tuhan Yang Maha Esa, penulis dapat menyelesaikan Laporan Skripsi yang berjudul “Implementasi Virtual Private Network (VPN) Server Menggunakan Mikrotik Untuk Remote Access Di SMK Islam Manbaul Hikmah Luwunragi” sesuai dengan yang direncanakan. Selanjutnya penulis menyampaikan terima kasih kepada :

1. Bapak Rektor Universitas Muhadi Setiabudi Dr. Roby Setiadi, S.Kom, M.M
2. Bapak Abdul Khamid, ST, MT, selaku Dekan Fakultas Teknik dan selaku Dosen Pembimbing II yang telah memberikan dukungan sehingga penulisan Laporan Skripsi ini terselesaikan
3. Bapak Agystia Premana S.Kom, M.Kom selaku ketua Program Studi Teknik Informatika sekaligus Dosen Pembimbing I yang telah membimbing dengan baik
4. Bapak Nur Ariesanto Ramdhan, S.Kom, M.Kom selaku Dosen Wali yang selalu menginspirasi dan memberi motivasi kepada mahasiswa
5. Semua pihak yang memberikan dukungan dan bantuan kepada penulis baik secara langsung maupun tidak langsung

Semoga penulisan Laporan Skripsi ini dapat memberikan manfaat sekaligus menambah pengetahuan bagi berbagai pihak. Amin.

Brebes, 17 Agustus 2021

Penulis

DAFTAR ISI

	Halaman
HALAMAN JUDUL	i
HALAMAN PENGESAHAN.....	ii
TANDA PERSETUJUAN SEMINAR SKRIPSI	ii
TANDA PERSETUJUAN SIDANG SKRIPSI.....	iii
PERNYATAAN.....	vi
KATA PENGANTAR	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	x
DAFTAR TABEL	xii
DAFTAR LAMPIRAN	xiii
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah	3
1.3. Tujuan Penelitian	3
1.4. Manfaat Penelitian	3
1.5. Ruang Lingkup Penelitian	4
1.6. Batasan Masalah	4
1.7. Sistematika Penulisan.....	4
BAB II TINJAUAN PUSTAKA.....	6
2.1. Konsep Dasar Jaringan.....	6
2.2. Topologi Jaringan.....	10
2.2.1 Topologi Bus	10
2.2.2 Topologi Ring	11
2.2.3 Topologi Star	12
2.2.4 Topologi Mesh.....	13
2.2.5 Topologi Tree	14
2.3. IP Address	15
2.4. Virtual Private Network.....	17
2.4.1 Pengertian VPN.....	17
2.4.2 Cara Kerja VPN.....	19
2.4.3 Keuntungan dan kekurangan VPN	20
2.4.4 Manfaat dan Kegunaan VPN.....	21
2.4.5 Tipe VPN	23
2.5. Enkripsi	27
2.6. Mikrotik.....	28
2.6.1 Pengertian Mikrotik.....	28
2.6.2 Fitur Mikrotik.....	31
BAB III METODE PENELITIAN.....	33
3.1. Penelitian Terkait.....	33

3.1.1 Hendra Supendar (2016).....	33
3.1.2 E. Mufida, D. Irawan dan G. Chrisnawati (2017)	34
3.1.3 Fitri Sjafrina, Pipit Dewi Arnesia dan Arif Aqim (2019)	36
3.1.4 Puputro Sanzoyo Utomo (2020).....	38
3.2. Permasalahan Sistem Jaringan.....	39
3.3. Analisa Penelitian	39
3.2.1 Alat dan Kebutuhan Bahan.....	40
3.2.2 Desain	41
3.2.3 Pengujian	42
3.4. Metode Pengumpulan Data.....	43
3.3.1 Observasi	43
3.3.2 Wawancara	43
3.3.3 Studi Pustaka	44
3.5. Kerangka Berpikir	45
BAB IV IMPLEMENTASI SISTEM	47
4.1 Simulasi Topologi Jaringan	47
4.2 Konfigurasi Mikrotik.....	47
4.3 Konfigurasi VPN PPTP	57
4.4 Pengujian Jaringan	65
4.5 Pengujian Jaringan Akhir	67
BAB V KESIMPULAN DAN SARAN	70
5.1 Kesimpulan.....	70
5.2 Saran.....	70
DAFTAR PUSTAKA.....	72
LAMPIRAN.....	74

DAFTAR GAMBAR

	Halaman
Gambar 2. 1 Local Area Network (LAN)	6
Gambar 2. 2 Metropolitan Area Network (MAN)	7
Gambar 2. 3 Wide Area Network (WAN)	7
Gambar 2. 4 Jaringan Client Server.....	9
Gambar 2. 5 Jaringan Peer-to-Peer	9
Gambar 2. 6 Topologi Bus	11
Gambar 2. 7 Topologi Ring	12
Gambar 2. 8 Topologi Star	13
Gambar 2. 9 Topologi Mesh	14
Gambar 2. 10 Topologi Tree	15
Gambar 2. 11 Konsep VPN	18
Gambar 2. 12 Tipe Site-to-site	24
Gambar 2. 13 Tipe Remote Access	25
Gambar 2. 14 Mikrotik RB-941 2nd TC.....	30
Gambar 2. 15 Tampilan utama Winbox	31
Gambar 3. 1 Tampilan Aplikasi Winbox	41
Gambar 3. 2 Desain Topologi Jaringan VPN	42
Gambar 3. 3 Transfer Rate VPN.....	43
Gambar 4. 1 Desain Topologi Jaringan VPN	47
Gambar 4. 2 Menjalankan aplikasi Winbox.....	48
Gambar 4. 3 Pengaturan IP Address	48
Gambar 4. 4 Pengaturan Route Table	49
Gambar 4. 5 Pengaturan Nat.....	50
Gambar 4. 6 Pengaturan IPSec Peer	50
Gambar 4. 7 Pengaturan IPSec Policy	51
Gambar 4. 8 Pengaturan IPSec Proposal	51
Gambar 4. 9 Pengaturan IP Address	52
Gambar 4. 10 Pengaturan Route Table	53
Gambar 4. 11 Pengaturan Nat.....	54
Gambar 4. 12 Pengaturan IPSec Peer	55
Gambar 4. 13 Pengaturan IPSec Policy	56
Gambar 4. 14 Pengaturan IPSec Proposal.....	56
Gambar 4. 15 Enable PPTP Server	58
Gambar 4. 16 New PPP Secret Server.....	59

Gambar 4. 17 Dial Out PPTP.....	60
Gambar 4. 18 Penambahan static route di Router SMK	60
Gambar 4. 19 Penambahan static route di Router Rumah	61
Gambar 4. 20 PPP Secret Client	61
Gambar 4. 21 Set up new connection or network.	62
Gambar 4. 22 Connect to a workplace.....	62
Gambar 4. 23 Use My Internet Connection (VPN)	63
Gambar 4. 24 Connect Interface VPN	63
Gambar 4. 25 Connect Workspace Client.....	64
Gambar 4. 26 Autentikasi VPN	64
Gambar 4. 27 Ping dari Client ke Gateway pada Kantor SMK.....	65
Gambar 4. 28 Ping dari Client ke Router pada Kantor SMK	66
Gambar 4. 29 Analisa sebelum menggunakan VPN.....	66
Gambar 4. 30 Ping dari client kantor SMK ke router Rumah	67
Gambar 4. 31 Ping dari client SMK ke client rumah.....	67
Gambar 4. 32 Tes Tracert dari SMK ke rumah	68
Gambar 4. 33 Grafik Transfer Data pada Router Pusat.....	68
Gambar 4. 34 Grafik Transfer Data pada Router Cabang	69
Gambar 4. 35 Analisa Paket Data.....	69

DAFTAR TABEL

	Halaman
Tabel 2. 1 Jaringan Komputer Berdasarkan Area	8
Tabel 3. 1 Kebutuhan Perangkat Keras	40

DAFTAR LAMPIRAN

	Halaman
Lampiran 1 Surat Keterangan Penelitian	74
Lampiran 2 Lembar Wawancara	75
Lampiran 3 Dokumentasi Penelitian	76

IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN) SERVER MENGUNAKAN MIKROTIK UNTUK REMOTE ACCESS DI SMK ISLAM MANBAUL HIKMAH LUWUNGRAGI

ABSTRAK

Dengan adanya kebutuhan mengakses jaringan lokal dari rumah dengan aman, sekolah sebagai lembaga pengelola informasi tentunya harus mampu mengamankan lalu lintas dari sebuah data yang terdapat pada jaringan komputer. Secara umum VPN adalah suatu proses dimana jaringan umum atau internet diamankan untuk memfungsikan sebagai jaringan pribadi (*private network*). Selain sebagai teknologi untuk memperlancar arus transfer data dan informasi, VPN juga penting untuk mengamankan keberadaan data tersebut agar tidak disalahgunakan. VPN memungkinkan pengguna mampu terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dengan jaringan lokal. Pemasangan VPN di SMK Islam Manbaul Hikmah Luwungragi menggunakan server mikrotik *router operating system*. Data yang berjalan di dalam sebuah tunnel tidak dapat dimonitor karena data tersebut telah mengalami kompresi dan enkripsi. Pemanfaatan Virtual Private Network (VPN) yang dapat membangun koneksi pada jaringan *public* (internet) dengan hak dan pengaturan seperti pada jaringan lokal dapat dijadikan pilihan sebagai sarana pengaksesan file serta kontrol jarak jauh (*remote*) pada server secara cepat dan praktis.

Kata Kunci : *Jaringan Komputer, Virtual Private Network, VPN, Mikrotik, Remote Acces*

**IMPLEMENTATION OF VIRTUAL PRIVATE NETWORK (VPN) SERVER
USING MICROTİK FOR REMOTE ACCESS AT SMK ISLAM MANBAUL
HIKMAH LUWUNGRAGI**

ABSTRACT

The need to access the local network from home safely, schools as information management institutions must of course be able to secure traffic from data contained on computer networks. In general, VPN is a process where a public network or internet is secured to function as a private network. Apart from being a technology to facilitate the flow of data and information transfer, VPN is also important to secure the existence of the data so that it is not misused. VPNs allow users to be able to connect to public networks and use them to join local networks. VPN installation at Manbaul Hikmah Luwungragi Islamic Vocational School using a mikrotik server operating system router. Data running in a tunnel cannot be monitored because the data has been compressed and encrypted. Utilization of a Virtual Private Network (VPN) that can establish a connection on a public network (internet) with rights and settings such as on a local network can be chosen as a means of accessing files and remote control (remote) on the server quickly and practically.

Keywords : *Computer Network, Virtual Private Network, VPN, Mikrotik, Remote Acces*

BAB I

PENDAHULUAN

1.1. Latar Belakang

Industri 4.0 jaringan komputer sangatlah penting dalam menunjang komunikasi di berbagai sektor termasuk pendidikan. Banyak keuntungan yang dapat diperoleh dari penggunaan jaringan komputer, misalnya komunikasi antara guru dan siswa menjadi lebih mudah dan cepat melalui jaringan komputer atau juga untuk aplikasi *client-server* di dalam sebuah instansi. Pertukaran data yang awal mulanya hanya melalui *hard copy* berupa tulisan tangan, dokumen, laporan harian, bulanan maupun tahunan melalui media flashdisk dan sebagainya, telah berkembang menjadi komunikasi menggunakan jaringan internet karena tuntutan waktu dan efisiensi. Internet merupakan interkoneksi jaringan komputer skala besar yang dihubungkan menggunakan protokol khusus. WAN (*Wide Area Network*) dan LAN (*Local Area Network*) sudah mampu menghubungkan semua jaringan komputer yang ada di lokal ataupun di pusat. Dibalik kecanggihannya pemanfaatan teknologi dan internet harus didukung dengan canggihnya infrastruktur komunikasi yang dimiliki suatu lembaga pendidikan salah satunya adalah Virtual Private Network (VPN).

Secara umum VPN adalah suatu proses dimana jaringan umum atau internet diamankan untuk memfungsikan sebagai jaringan pribadi (*private network*). Selain sebagai teknologi untuk memperlancar arus transfer data dan informasi, VPN juga penting untuk mengamankan keberadaan data tersebut agar tidak disalahgunakan.

SMK Islam Manbaul Hikmah Luwunragi merupakan Sekolah Kejuruan yang berdiri pada tanggal 13 April 2015 dengan jurusan Teknik Bisnis Sepeda Motor dan jurusan Teknik Komputer Jaringan. Sejak berdiri SMK Islam Manbaul Hikmah selalu mengalami perkembangan. Sebagai wujud peningkatan mutu dan pelayanan Mulai tahun 2018 sekolah telah Terakreditasi dari Badan Akreditasi Nasional Sekolah dan Madrasah. Dan pada tahun 2019 sekolah telah menyandang predikat Mikrotik Academy,

yaitu suatu Instansi / Sekolah / perusahaan yang telah mengikat Kerjasama dengan Perusahaan Mikrotik Ls dari Latvia dalam bidang kurikulum pengetahuan dan penggunaan perangkat keras Mikrotik dalam penunjang pembelajaran. SMK Islam Manbaul Hikmah Luwungragi menggunakan internet sebagai media penyalur data dan pendukung kegiatan guru dan siswa dalam berkomunikasi dan penunjang pembelajaran.

Dengan adanya kebutuhan mengakses jaringan lokal dari rumah dengan aman, sekolah sebagai lembaga pengelola informasi tentunya harus mampu mengamankan lalu lintas dari sebuah data yang terdapat pada jaringan komputer, karena data tersebut bersifat rahasia yang hanya bisa diakses oleh orang-orang tertentu. SMK Islam Manbaul Hikmah Luwungragi memilih menggunakan VPN sebab akses informasi dapat berlangsung secara cepat, efektif dan lebih aman. Sedangkan jaringannya dapat diterapkan pada LAN (*Local Area Network*) dan WAN (*Wide Area Network*).

VPN memungkinkan pengguna mampu terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dengan jaringan lokal. Pemasangan VPN di SMK Islam Manbaul Hikmah Luwungragi menggunakan server mikrotik *router operating system*. Dengan mikrotik tersebut, SMK Islam Manbaul Hikmah Luwungragi dapat melakukan perbandingan antara layanan VPN dengan layanan tanpa VPN. Keduanya dapat diimplementasikan dengan menggunakan protokol IP Security, data yang berjalan di dalam sebuah tunnel tidak dapat dimonitor karena data tersebut telah mengalami kompresi dan enkripsi. Pemanfaatan Virtual Private Network (VPN) yang dapat membangun koneksi pada jaringan *public* (internet) dengan hak dan pengaturan seperti pada jaringan lokal dapat dijadikan pilihan sebagai sarana pengaksesan file serta kontrol jarak jauh (remote) pada server secara cepat dan praktis.

Berdasarkan uraian diatas, penulis mengimplementasikan Virtual Private Network (VPN) server menggunakan mikrotik untuk *remote access* di SMK Islam Manbaul Hikmah Luwungragi agar memudahkan

akses/koneksi kedalam jaringan lokal yang dapat diakses dari luar dengan cepat, efektif dan lebih aman.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka rumusan masalah yang akan dikaji adalah:

1. Bagaimana merancang suatu jaringan VPN menggunakan Mikrotik untuk SMK Islam Manbaul Hikmah Luwunragi yang aman
2. Bagaimana mengimplementasikan jaringan VPN sebagai sarana pengaksesan file serta kontrol jaringan jarak jauh di SMK Islam Manbaul Hikmah Luwunragi

1.3. Tujuan Penelitian

Berdasarkan latar belakang yang telah diuraikan diatas yang menjadi maksud dan tujuan penelitian ini adalah sebagai berikut:

1. Untuk mengimplementasikan suatu layanan yang berbasis Remote Access VPN di SMK Islam Manbaul Hikmah Luwunragi
2. Membangun infrastruktur jaringan untuk kemudahan akses/koneksi kedalam jaringan lokal (*intranet*) yang dapat diakses dari luar dengan aman

1.4. Manfaat Penelitian

Manfaat yang diperoleh dari penelitian ini adalah :

1. Bagi Instansi
Manfaat yang akan didapat oleh instansi adalah dapat menjadi sarana atau media informasi yang lebih handal dan aman dalam mengirim data atau informasi penting sebuah instansi sekolah
2. Bagi Peneliti
Manfaat yang didapat bagi peneliti adalah dapat menjadi sebuah acuan untuk penelitian lebih lanjut demi memperoleh hasil yang

maksimal dan menerapkan ilmu yang didapat dari kampus maupun di luar kampus agar menjadi ilmu yang bermanfaat

1.5. Ruang Lingkup Penelitian

Adapun ruang lingkup dalam penelitian ini adalah :

1. Fokus dalam penelitian ini membahas implementasi Virtual Private Network (VPN) menggunakan perangkat *router* Mikrotik. Adapun perangkat lain yang berkaitan dengan penelitian ini adalah perangkat pendukung yang tidak termasuk dalam pembahasan.
2. Terdapat banyak teknik yang digunakan dalam VPN, pada penelitian ini penulis menggunakan teknik PPTP Tunnel (*Point To Point Tunneling Protocol*) yang disesuaikan dengan kebutuhan lapangan
3. Untuk mengimplementasikan suatu layanan yang berbasis remote access VPN dengan Metode PPTP yang bertujuan sebagai salah satu optimalisasi jaringan di SMK Islam Manbaul Hikmah Luwungragi

1.6. Batasan Masalah

Agar permasalahan lebih terarah dan tidak menyimpang dari permasalahan yang akan dibuat perlu adanya batasan masalah diantaranya:

1. Merancang Remote Site Virtual Private Network (VPN) menggunakan sistem operasi mikrotik router dan perangkat RouterBoard.
2. Mengimplementasikan Remote Site Virtual Private Network (VPN) *site to site* berbasis PPTP.

1.7. Sistematika Penulisan

Penulisan Skripsi ini dibagi menjadi beberapa bagian :

BAB I Pendahuluan

Berisikan latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, ruang lingkup penelitian, dan batasan masalah

BAB II Tinjauan Pustaka

Berisikan teori-teori yang mendasari skripsi ini yaitu mengenai konsep dasar jaringan, VPN, Remote Access, Mikrotik dan parameter-parameter yang digunakan pada skripsi ini

BAB III Metode Penelitian

Membahas mengenai metode penelitian dan perancangan system yang akan digunakan serta instalasi dan konfigurasi system VPN Server, Remote Access, dan Mikrotik

BAB IV Implementasi Sistem

Berisi tentang penjelasan dan penerapan konfigurasi system yang digunakan

BAB V Kesimpulan dan Saran

Berisi kesimpulan dan saran yang didapat dari penelitian ini

BAB II

TINJAUAN PUSTAKA

2.1. Konsep Dasar Jaringan

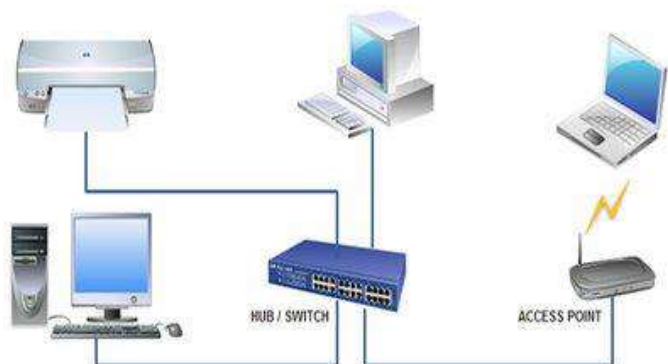
Dengan semakin berkembangnya kebutuhan pengolahan data dan informasi, di dalam sebuah perusahaan dibutuhkan beberapa komputer yang digunakan oleh banyak orang yang bekerja dalam sebuah tim. Untuk saling bertukar data dan informasi, maka komputer-komputer yang digunakan akan terhubung antara satu dengan yang lainnya. Kumpulan komputer yang saling terhubung disebut sebagai jaringan komputer.

Jaringan komputer merupakan kumpulan dari beberapa komputer yang dihubungkan satu dengan lainnya dengan menggunakan protokol komunikasi. Jaringan ini memerlukan media transmisi tertentu untuk dapat saling berbagi informasi, program, dan penggunaan bersama perangkat keras.

Berdasarkan skala atau area, Jaringan komputer dapat terbagi menjadi 4, yaitu:

1. Local Area Network (LAN)

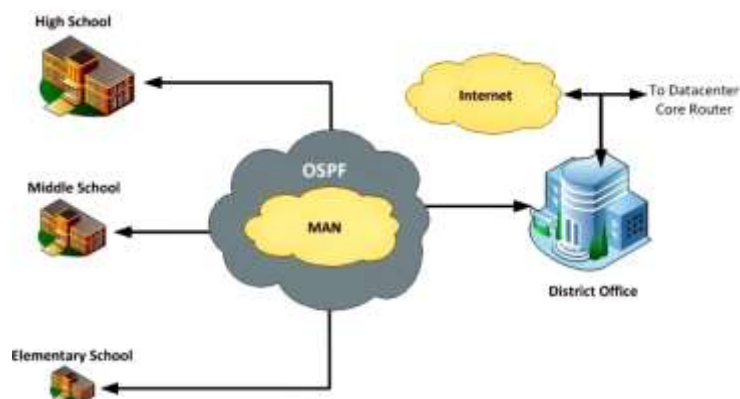
Local Area Network (LAN) adalah jaringan lokal yang dibuat pada area terbatas. Misalnya dalam satu gedung atau dalam satu ruangan. Kadang kala jaringan lokal disebut juga jaringan personal atau privat. LAN biasa digunakan pada sebuah jaringan kecil yang menggunakan resource secara bersama, seperti penggunaan printer secara bersama, penggunaan media penyimpanan secara bersama, dan sebagainya.



Gambar 2. 1 Local Area Network (LAN)

2. Metropolitan Area Network (MAN)

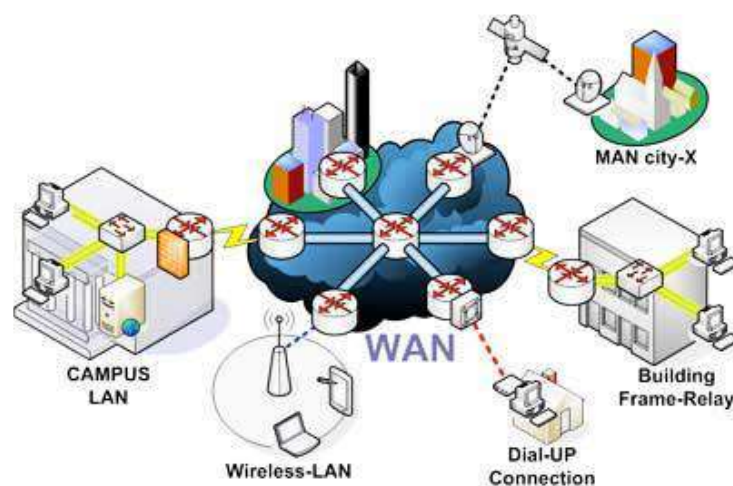
Metropolitan Area Network adalah jaringan komputer yang cakupannya lebih luas dibandingkan LAN. Kategori ini dapat dikatakan gabungan dari beberapa jaringan LAN. Cakupan lokasinya mencapai satu atau lebih dari suatu kota. MAN biasanya digunakan untuk menghubungkan kantor-kantor perusahaan yang berdekatan dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum.



Gambar 2. 2 Metropolitan Area Network (MAN)

3. Wide Area Network (WAN)

Wide Area Network (WAN) Wide Area Network adalah jaringan komputer yang mencakup daerah geografis yang luas, sering kali mencakup sebuah negara atau benua.



Gambar 2. 3 Wide Area Network (WAN)

4. Internet

Internet (Interconnection Networking) adalah seluruh jaringan komputer yang saling terhubung menggunakan standar sistem global Transmission Control Protocol/Internet Protocol Suite (TCP/IP) sebagai protokol pertukaran paket (packet switching communication protocol) untuk melayani miliaran pengguna di seluruh dunia, bahkan antar planet.

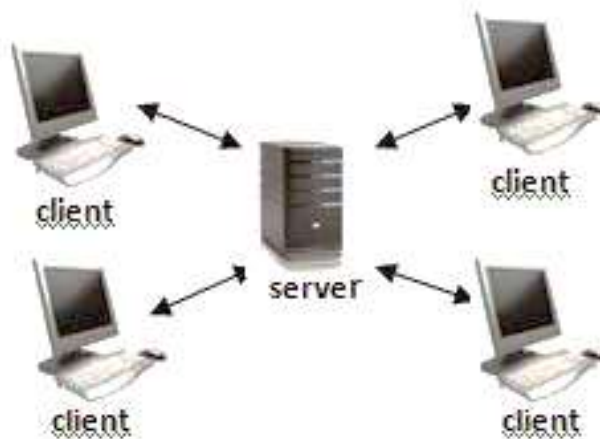
Tabel 2. 1 Jaringan Komputer Berdasarkan Area

Jarak/cakupan (meter)	Contoh	Jenis
10-100	Ruangan	LAN
100-1.000	Gedung	LAN
1000-10.000	Kampus	LAN
10.000-100.000	Kota	MAN
100.000-1.000.000	Negara	WAN
1.000.000-10.000.000	Benua	WAN

Berdasarkan pola operasi atau fungsinya, jaringan komputer dapat dibagi menjadi 2 jenis, yaitu:

1. Client Server

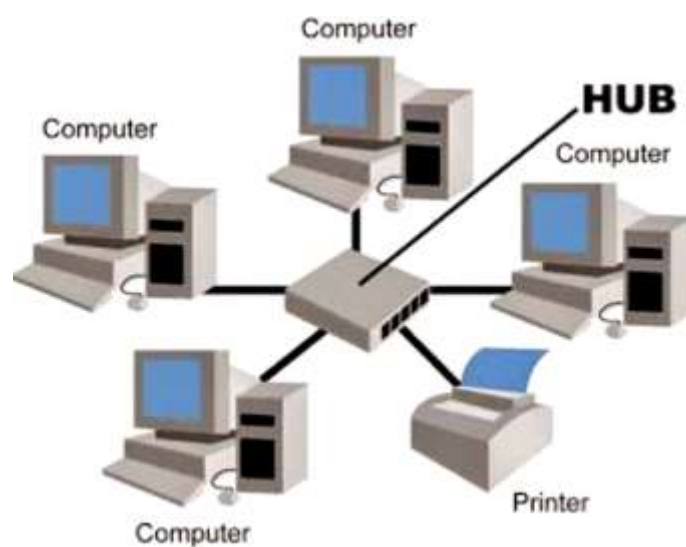
Client Server adalah jaringan komputer yang mengharuskan salah satu (atau lebih) komputer difungsikan sebagai server atau central. Server melayani komputer lain yang disebut client. Layanan yang diberikan bisa berupa akses Web, e-mail, file, atau yang lain. Client Server banyak dijumpai pada jaringan Internet. Namun LAN atau jaringan lain pun bisa mengimplementasikan client server. Hal ini sangat bergantung pada kebutuhan masing-masing.



Gambar 2. 4 Jaringan Client Server

2. Peer to Peer

Sistem operasi jaringan model Peer-to-Peer memungkinkan seorang pemakai jaringan computer membagi sumber daya yang ada dikomputernya, baik itu file data, printer dan mengakses sumber daya computer yang lainnya. Adapun gambar topologi Peer-to-Peer. Model ini tidak mempunyai sebuah file server atau induk server yang terpusat, seluruh komputer memiliki kemampuan atau hak yang sama untuk memakai sumber daya yang tersedia di jaringan komputer tersebut.



Gambar 2. 5 Jaringan Peer-to-Peer

2.2. Topologi Jaringan

Topologi jaringan merupakan gambaran pola hubungan antara komponen-komponen jaringan, yang meliputi komputer server, komputer client/workstation, hub/switch, pengkabelan dan komponen jaringan yang lain. Topologi fisik menguraikan layout aktual dari perangkat keras (hardware) jaringan, sedangkan topologi logika menguraikan perilaku komputer pada jaringan dari sudut pandang operator manusianya (brainware).

Topologi itu sendiri mempunyai kelebihan dan kekurangan. Berikut penjelasan dari masing-masing topologi :

2.2.1 Topologi Bus

Topologi Bus merupakan topologi yang menghubungkan beberapa komputer ke sebuah kabel dengan beberapa terminal. Topologi Bus menggunakan jenis kabel Coaxial dengan beberapa konektor BNC.

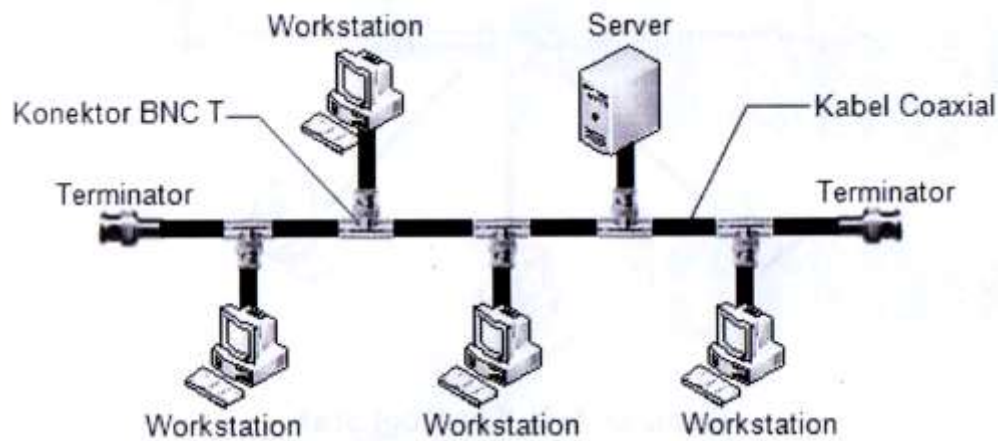
Topologi Bus merupakan arsitektur jaringan dimana client-client yang ada di jaringan dihubungkan melalui line komunikasi yang ter-share yang disebut bus.

Keuntungan :

- a. Hemat kabel
- b. layout kabel sederhana
- c. Setiap komputer dapat saling berhubungan langsung.

Kerugian :

- a. Kepadatan lalu lintas data
- b. Sering terjadi hang (*crass talk*) ketika lebih dari satu pasang memakai jalur di waktu yang sama.



Gambar 2. 6 Topologi Bus

2.2.2 Topologi Ring

Topologi Ring merupakan topologi yang menghubungkan beberapa komputer dengan membentuk lingkaran. Komputer yang terhubung dalam sebuah jaringan akan terkoneksi pada 2 komputer lain.

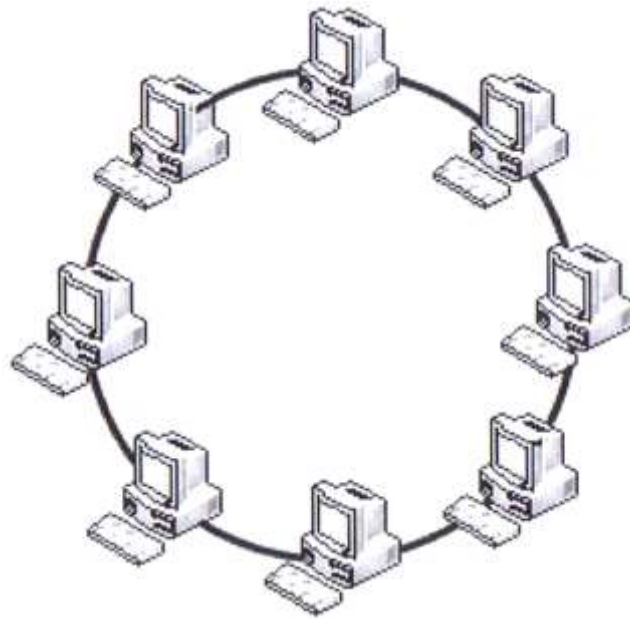
Setiap informasi yang diperoleh diperiksa alamat-alamatnya oleh terminal yang dilewati. Jika informasi itu bukan untuknya maka informasi itu di putar lagi sampai menemukan alamat yang benar. Setiap terminal LAN saling bergantung, sehingga jika terjadi kerusakan satu terminal saja, keseluruhan LAN akan terganggu. Media koneksi yang digunakan adalah kabel UTP cat 3.

Keuntungan:

- a. Laju data tinggi
- b. Dapat melayani lalu lintas yang padat
- c. Komunikasi antar terminal yang mudah

Kerugian:

- a. Kerusakan pada satu terminal melumpuhkan jaringan.
- b. Bila ada kerusakan pada media pengiriman data dapat menghentikan kerja seluruh jaringan.



Gambar 2. 7 Topologi Ring

2.2.3 Topologi Star

Topologi Star merupakan topologi yang menghubungkan beberapa komputer dengan menggunakan perangkat yaitu Hub atau Switch.

Dengan menggunakan topologi jenis ini maka jaringan mudah dikembangkan dengan menarik kabel ke konsentrator atau node pusat. Media koneksi yang digunakan adalah kabel UTP (10/100/1000Base-T).

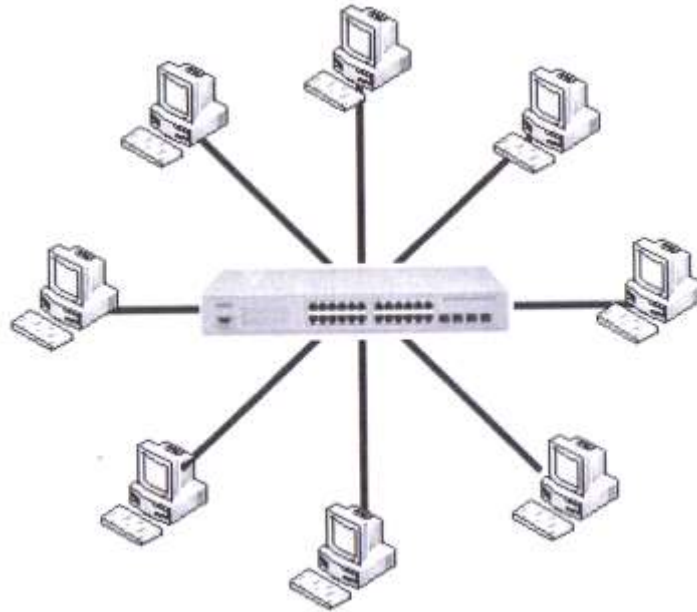
Keuntungan:

- a. Paling fleksibel
- b. Pemasangan atau perubahan stasiun sangat mudah dan tidak mengganggu bagian jaringan lain.
- c. Kemudahan deteksi dan isolasi kesalahan atau kerusakan

Kerugian:

- a. Boros kabel

- b. Perlu penanganan khusus
- c. Kontrol terpusat (HUB, Switch) jadi elemen kritis



Gambar 2. 8 Topologi Star

2.2.4 Topologi Mesh

Topologi mesh merupakan topologi jaringan yang pada semua titik terminal saling terhubung dengan titik yang lain, sehingga membentuk jaringan yang kompleks.

Pada topologi Full Mesh, setiap komponen jaringan memiliki hubungan langsung atau jalur khusus ke setiap komponen jaringan yang lain dalam segmen tersebut. Jika satu saja dari jalur khusus tersebut dihilangkan, maka topologi yang terbentuk tidak dapat lagi disebut Full Mesh melainkan menjadi partial Mesh.

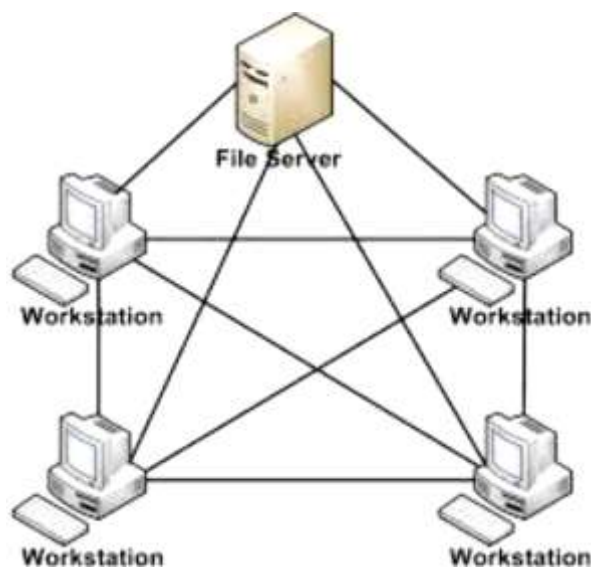
Keuntungan:

- a. Pengiriman data, dari satu node ke sejumlah simpul yang lain dapat dilakukan secara bersamaan.
- b. Pemecahan masalah lebih mudah dibandingkan dengan topologi jaringan komputer lainnya.

- c. Jika ada ekspansi jaringan, tidak akan menyebabkan gangguan pada pengguna jaringan lainnya.

Kekurangan:

- a. Membutuhkan lebih banyak perangkat keras jaringan (misalnya: kabel jaringan, dan lain-lain) dibandingkan dengan topologi yang lainnya.
- b. Pelaksanaan (instalasi dan konfigurasi) topologi ini sangat rumit dan mungkin sangat berantakan. Sejumlah besar input atau output port diperlukan.
- c. Biaya instalasi dan pemeliharaan jaringan komputer mesh cukup tinggi.



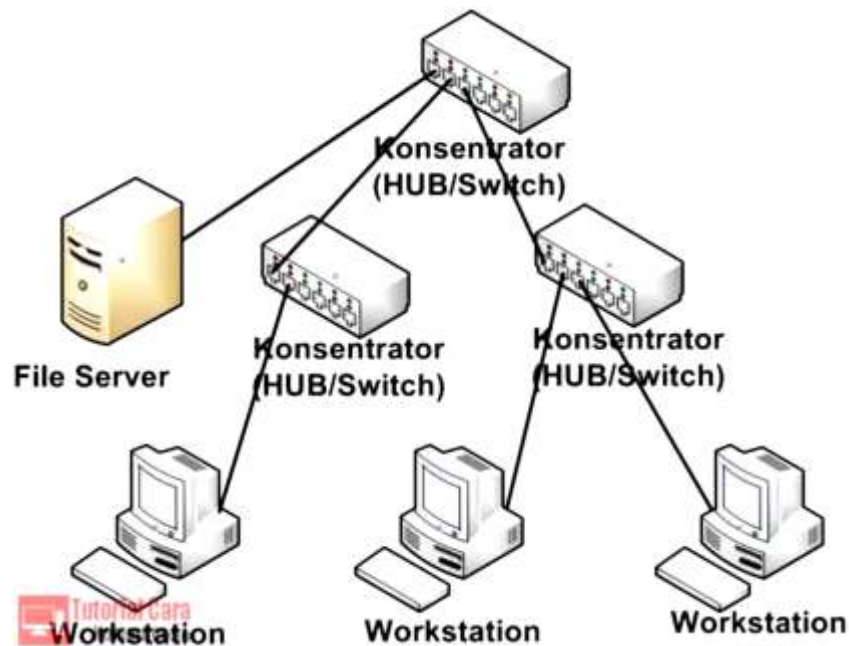
Gambar 2. 9 Topologi Mesh

2.2.5 Topologi Tree

Topologi tree merupakan gabungan beberapa topologi star yang dihubungkan dengan topologi bus. Topologi tree digunakan untuk menghubungkan beberapa LAN dengan LAN lain. Hubungan antara LAN dilakukan via hub. Masing-masing hub dapat dianggap sebagai akar (root) dari masing-masing pohon (tree).

Topologi tree dapat mengatasi kekurangan topologi bus yang disebabkan persoalan broadcast traffic, dan kekurangan topologi star yang disebabkan oleh keterbatasan kapasitas port hub.

Karakteristik yang dimiliki topologi tree mirip dengan topologi bus dan star. Begitu juga dengan peralatan, kabel, dan teknik pemasangan.



Gambar 2. 10 Topologi Tree

2.3. IP Address

IP (Internet Protocol) Address merupakan alamat yang diberikan kepada komputer-komputer yang terhubung dalam suatu jaringan. IP Address terdiri dari dua bagian, yaitu: Network ID dan Host ID.

Lima fungsi utama IP Address yaitu:

1. Mendefinisikan paket yang menjadi unit satuan terkecil pada transmisi data di Internet.
2. Memindahkan data antara Transport Layer dan Network Interface Layer.
3. Mendefinisikan skema pengalamatan Internet atau IP address.

4. Menentukan routing paket.
5. Melakukan fragmentasi dan penyusunan ulang paket.

IP Address berdasarkan perkembangannya dibagi menjadi dua jenis yaitu:

1. IPv4 (Internet Protocol versi 4)
merupakan IP Address yang terdiri dari 32 bit yang dibagi menjadi 4 segmen berukuran 8 bit.
2. IPv6 (Internet Protocol versi 6)
merupakan IP Address yang terdiri dari 128 bit yang digunakan untuk mengatasi permintaan IP Address yang semakin meningkat.

IP Address terdiri dari 32 bit angka biner yang dituliskan dalam bentuk empat kelompok dan masing-masing kelompok terdiri dari delapan (oktat) bit yang dipisahkan oleh tanda titik.

Contoh: 11000000.10101000.00000000.01100100

IP Address dapat juga ditulis dalam bentuk angka desimal dalam empat kelompok, dari angka 0-255.

Contoh : 192.168.0.100

Untuk memudahkan pengaturan IP address seluruh komputer pengguna jaringan internet, dibentuklah suatu badan yang mengatur pembagian IP address. Badan tersebut bernama InterNIC (Internet Network Information Center). InterNIC membagi-bagi IP address menjadi beberapa kelas. Kelas-kelas tersebut meliputi:

1. Kelas A

IP kelas A terdiri dari 8 bit pertama digunakan untuk Network ID, dan 24 bit berikutnya merupakan Host ID. IP kelas A memiliki 126 Network, yaitu dari nomor 1.xxx.xxx.xxx sampai dengan 126.xxx.xxx.xxx (xxx merupakan variabel yang nilainya dari 0 sampai dengan 255).

2. Kelas B

IP kelas B terdiri dari 16 bit pertama digunakan untuk Network ID, dan 16 bit berikutnya merupakan Host ID. IP kelas B memiliki 16.384 network, yaitu dari nomor 128.0.xxx.xxx sampai dengan 191.255.xxx.xxx.

3. Kelas C

IP kelas C terdiri dari 24 bit pertama digunakan untuk Network ID, dan 8 bit berikutnya merupakan Host ID. IP kelas C memiliki 2.097.152 network, yaitu dari nomor 192.0.0.xxx sampai dengan 223.255.255.xxx.

2.4. Virtual Private Network

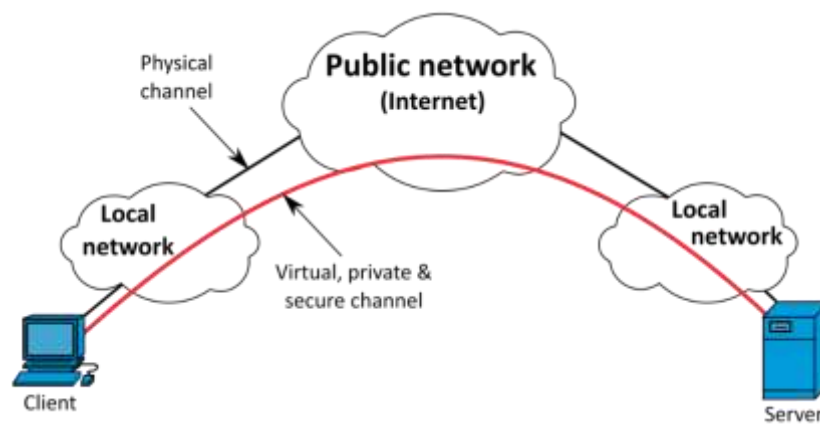
2.4.1 Pengertian VPN

Jika dibahas dari masing-masing kata dari VPN, yaitu : Virtual, Private dan Network, maka akan diperoleh arti sebagai berikut :

1. Virtual (Tidak nyata), tidak nyata, tidak tampak fisik.
2. Private (Privat), terlindungi, tidak dapat di akses dari luar
3. Network (Jaringan), sekumpulan alat-alat jaringan yang saling berkomunikasi satu dengan yang lain melalui beberapa metode arbitrary (berubah-ubah).

Sehingga Virtual Private Network (VPN) merupakan suatu cara untuk membuat sebuah jaringan bersifat private dan aman dengan menggunakan jaringan komputer misalnya internet. VPN dapat mengirim data antara dua komputer yang melewati jaringan publik sehingga seolah-olah terhubung secara point to point, meskipun sebenarnya data melewati jaringan publik. Dengan cara tersebut akan didapatkan hak dan pengaturan yang sama seperti halnya berada di dalam jaringan lokal, walaupun sebenarnya menggunakan jaringan internet.

Secara umum, VPN adalah sebuah proses dimana jaringan umum (public network atau internet) diamankan kemudian difungsikan menjadi sebuah jaringan privat (private network). Sebuah VPN tidak didefinisikan oleh rangkaian khusus atau router, tetapi didefinisikan oleh mekanisme keamanan dan prosedur-prosedur yang hanya mengizinkan penggunaanya yang ditunjuk akses ke VPN dan informasi yang mengalir melaluinya. Berikut adalah gambaran mengenai konsep dasar dari VPN.



Gambar 2. 11 Konsep VPN

Suatu organisasi atau institusi dalam melangsungkan kegiatannya tidak akan lepas dari pertukaran informasi antar para stakeholder yang satu dengan yang lain. Setiap informasi yang dihasilkan oleh salah satu stakeholder akan diperlukan oleh stakeholder lain. Untuk itu, kebutuhan informasi harus dapat diakses melalui jaringan komputer yang di desain untuk dapat mendapatkan informasi yang diperlukan dengan cepat, mudah, aman dan akurat. Dalam sebuah jaringan komputer, keamanan sewaktu pengiriman dan penerimaan data sangat penting untuk menjamin bahwa data yang dikirim sampai pada yang pihak yang dituju, dan tidak jatuh pada pihak yang tidak berkepentingan, terutama apabila data yang dikirimkan tersebut bersifat rahasia. Untuk itu perlu dilakukan pengamanan data pada jaringan dengan

menggunakan metode-metode tertentu. Salah satu cara untuk mengamankan data pada suatu jaringan adalah dengan mengimplementasikan VPN yang dapat membuat sebuah jaringan bersifat private dan aman dengan menggunakan jaringan komputer atau internet.

VPN adalah sebuah teknologi jaringan komputer yang dikembangkan oleh perusahaan skala besar yang menghubungkan antar jaringan diatas jaringan lain menggunakan internet yang membutuhkan jalur privacy dalam komunikasinya. Sifat pribadi VPN berarti bahwa traffic data VPN yang pada umumnya tidak terlihat, atau di enkapsulasi oleh lalu lintas jaringan yang mendasarinya. Dalam istilah yang lebih teknis, di link lapisan protokol jaringan virtual dikatakan terowongan atau tunnel yang melewati jaringan transportasi yang mendasarinya. Istilah VPN dapat digunakan untuk menggambarkan berbagai macam konfigurasi jaringan dan protokol.

2.4.2 Cara Kerja VPN

Secara sederhana cara kerja VPN (dengan protokol PPTP) adalah sebagai berikut:

- a. VPN membutuhkan sebuah server yang berfungsi sebagai penghubung antar PC, Server VPN ini bisa berupa komputer dengan aplikasi VPN Server atau sebuah Router, misalnya MikroTik RB 941.
- b. Untuk memulai sebuah koneksi, komputer dengan aplikasi VPN Client mengontak Server VPN, VPN Server kemudian memverifikasi username dan password dan apabila berhasil maka VPN Server memberikan IP Address baru pada komputer client dan selanjutnya sebuah koneksi / tunnel akan terbentuk.
- c. Untuk selanjutnya komputer client bisa digunakan untuk mengakses berbagai resource (komputer atau LAN) yang

berada dibelakang VPN Server misalnya melakukan transfer data, ngeprint dokument, browsing dengan gateway yang diberikan dari VPN Server, melakukan remote desktop dan lain sebagainya

2.4.3 Keuntungan dan kekurangan VPN

Beberapa keuntungan dari teknologi VPN diantaranya adalah:

- a. Remote Access, dengan VPN kita dapat mengakses komputer atau jaringan kantor, dari mana saja selama terhubung ke internet
- b. Keamanan, dengan koneksi VPN kita bisa berselancar dengan aman ketika menggunakan akses internet publik seperti hotspot atau internet cafe.
- c. Menghemat biaya setup jaringan, VPN dapat digunakan sebagai teknologi alternatif untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif kecil, karena transmisi data teknologi VPN menggunakan media jaringan publik yang sudah ada tanpa perlu membangun jaringan pribadi.

Beberapa kekurangan dari VPN diantaranya adalah:

- a. Koneksi internet (jaringan publik) yang tidak bisa kita prediksi. Hal ini dapat kita maklumi karena pada dasarnya kita hanya "nebeng" koneksi pada jaringan pihak lain sehingga otomatis kita tidak mempunyai kontrol terhadap jaringan tersebut.
- b. Perhatian lebih terhadap keamanan. Lagi-lagi karena faktor penggunaan jaringan publik, maka kita perlu memberikan perhatian yang lebih untuk mencegah terjadinya hal-hal yang tidak diinginkan seperti penyadapan, hacking dan tindakan *cyber crime* pada jaringan VPN.

2.4.4 Manfaat dan Kegunaan VPN

VPN merupakan paket solusi komunikasi data (baik berupa data suara, video, atau file digital lainnya) yang memberikan layanan berbasis IP ke end user. Layanan VPN dapat mengirimkan data antar-dua komputer yang melewati jaringan publik, misalnya Internet, sehingga seolah-olah terhubung secara point-to-point.

Beberapa manfaat dan kegunaan VPN yaitu:

- a. Kemampuan membentuk jaringan LAN yang tidak di batasi tempat dan waktu, karena koneksitasnya dilakukan via internet. Koneksi internet apapun dapat digunakan seperti Dial-Up, ADSL, Cable Modem, WIFI, 3G, CDMA Net, GPRS, dan sistem PVN ini paling tepat digunakan untuk penggunaan suatu database terpusat untuk mengkomunikasikan antara server dan client via internet seperti Aplikasi Perdagangan, Purchase, P.O.S, Accounting, Cashir, Billing system dan General Ledger
- b. Tidak ada ketergantungan terhadap keharusan memiliki IP Publik yang berharga mahal. Cukup menggunakan IP dynamic saja dengan kata lain asal PC bisa berinternet .
- c. Mampu mencetak dokumen dari rumah ke kantor via internet.
- d. mampu melakukan transfer data atau remote view untuk mengendalikan komputer dirumah/kantor dimana saja
- e. Tidak membutuhkan Peralatan/hardware tambahan yang berfungsi sebagai IP forwarder/Port Forwarder yang menambah investasi.
- f. Dapat melakukan koneksitas dengan PC dikantor anda misalnya dengan memanfaatkan software yang bekerja di jaringan LAN seperti Citrix, Windows Terminal Server 2003, VNC, Radmin dan VOIP
- g. Dengan menggunakan software yang bekerja di jaringan LAN dapat melakukan pertukaran data secara langsung, Printing , Remote View, Mengatur administrasi PC, yang kesemua itu

dapat dilakukan dimanapun pengguna berada selama bisa terhubung ke internet

- h. Berselancar dengan aman ketika di akses internet publik / hotspot
- i. Jika perusahaan ingin mengoptimalkan biaya untuk membangun jaringan yang luas. Oleh karena itu VPN dapat digunakan sebagai teknologi alternatif untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif kecil, karena transmisi data teknologi VPN menggunakan media jaringan publik yang sudah ada.
- j. Jangkauan jaringan lokal yang dimiliki suatu perusahaan akan menjadi luas, sehingga perusahaan dapat mengembangkan bisnisnya di daerah lain. Waktu yang dibutuhkan untuk menghubungkan jaringan lokal ke tempat lain juga semakin cepat, karena proses instalasi infrastruktur jaringan dilakukan dari perusahaan / kantor cabang yang baru dengan ISP terdekat di daerahnya. penggunaan VPN secara tidak langsung akan meningkatkan efektivitas dan efisiensi kerja.
- k. Penggunaan VPN dapat mengurangi biaya operasional bila dibandingkan dengan penggunaan leased line sebagai cara tradisional untuk mengimplementasikan WAN.
- l. VPN dapat mengurangi biaya pembuatan jaringan karena tidak membutuhkan kabel (leased line) yang panjang. Penggunaan kabel yang panjang akan membutuhkan biaya produksi yang sangat besar. Semakin jauh jarak yang diinginkan, semakin meningkat pula biaya produksinya.
- m. VPN menggunakan internet sebagai media komunikasinya. Perusahaan hanya membutuhkan biaya dalam jumlah yang relatif kecil untuk menghubungkan perusahaan tersebut dengan pihak ISP (internet service provider) terdekat.
- n. VPN memberi kemudahan untuk diakses dari mana saja, karena VPN terhubung ke internet. Sehingga pegawai yang

mobile dapat mengakses jaringan khusus perusahaan di manapun dia berada. Selama dia bisa mendapatkan akses ke internet ke ISP terdekat, pegawai tersebut tetap dapat melakukan koneksi dengan jaringan khusus perusahaan

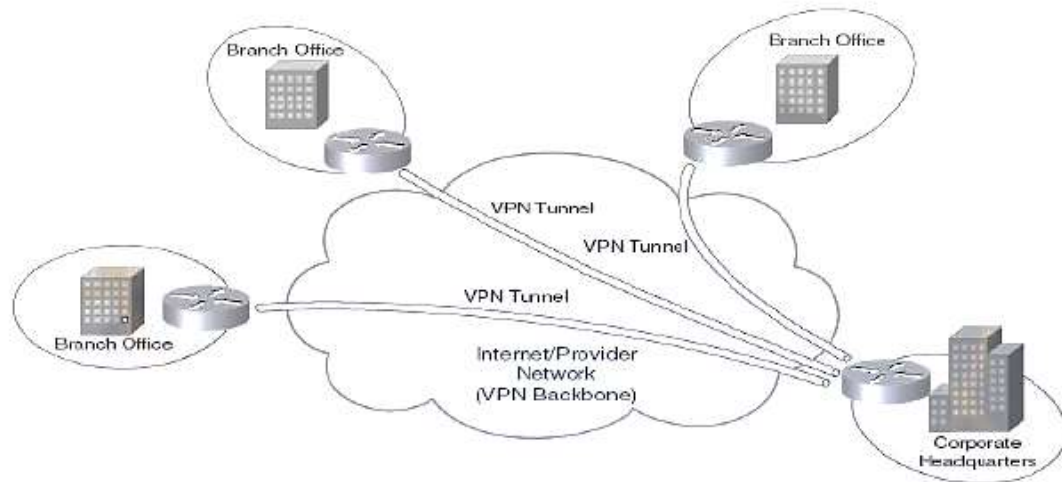
2.4.5 Tipe VPN

Secara garis besar tipe-tipe dalam teknologi VPN yang biasa yang digunakan adalah Site-to-site dan Remote Access.

1. Site-to-Site

Site-to-site dapat juga disebut LAN-to-LAN adalah berkomunikasi antar dua atau lebih jaringan area lokal (LAN) berbeda.

Suatu perusahaan pusat dengan cabangnya yang berkomunikasi dengan jarak yang berjauhan secara langsung oleh sebab itu dibangunlah VPN site-to-site sebagai solusi yang mutakhir. Bisa dibayangkan jika kantor pusat di Jakarta dan cabang di Surabaya jika dibuat jaringan lokalnya dengan menarik kabel fiber optic maka betapa besar biaya yang akan dikeluarkan. Site-to-site sering digunakan pada perusahaan kelas menengah keatas. Pada site-to-site protokol yang dapat digunakan adalah IP Security (Ipsec), Generic Routing Encapsulation (GRE), the Layer Two Tunneling Protocol version 3 (L2TPv3).



Gambar 2. 12 Tipe Site-to-site

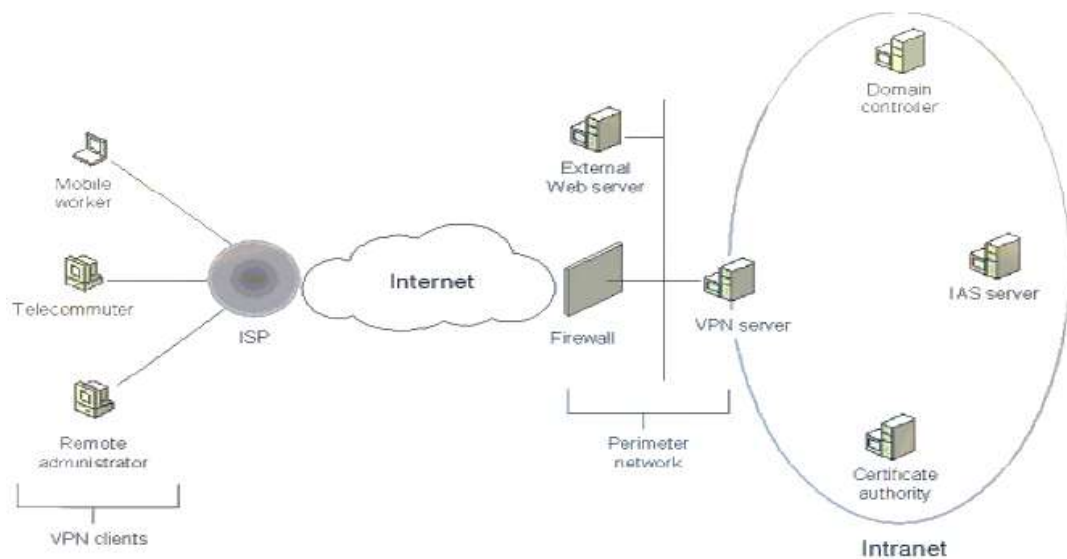
2. Remote Access

Remote access yang berarti akses dari jarak jauh merupakan suatu cara untuk manajemen server tanpa harus secara fisik menyentuh server dan melakukan manajemen di daerah operasional server. Remote access berguna untuk membuat pekerjaan bisa dilakukan di mana saja dan kapanpun selama ada akses jaringan ke server.

Remote access bisa dicapai dengan berbagai cara, yang pasti server yang di remote harus bisa diakses oleh host yang bersangkutan baik melalui jaringan internet lokal atau menggunakan VPN.

Salah satu remote access yang aman adalah menggunakan SSH (Secure Shell). SSH menyediakan koneksi untuk melakukan remote dengan aman dengan interface command line meskipun dengan jaringan yang tidak aman.

Aplikasi dari SSH ini biasanya digunakan untuk login sistem UNIX, untuk menggantikan sistem remote seperti telnet yang mengirim informasi password dengan tulisan biasa tanpa enkripsi.



Gambar 2. 13 Tipe Remote Access

Mikrotik support beberapa metode VPN seperti PPTP, L2TP, SSTP, dan OpenVPN. Dengan adanya beberapa opsi ini perlu memilih tipe VPN yang cocok untuk jaringan. Secara umum semua tipe tersebut memiliki fungsi yg sama. Yang membedakan adalah autentikasi dan enkripsi yg digunakan.

1. PPTP (Point to Point Tunnel Protocol)

PPTP merupakan salah satu type VPN yang paling sederhana dalam konfigurasi. Selain itu juga fleksibel. Mayoritas operating system sudah support sebagai PPTP Client, baik operating system pada PC ataupun gadget seperti android. Komunikasi PPTP menggunakan protokol TCP port 1723, dan menggunakan IP Protocol 47/GRE untuk enkapsulasi paket datanya. Pada setting PPTP bisa ditentukan network security protocol yang digunakan untuk proses autentikasi PPTP pada Mikrotik, seperti pap, chap, mschap dan mschap2. Kemudian setelah tunnel terbentuk, data yang ditransmisikan akan dienkripsi menggunakan Microsoft Point-to-Point Encryption (MPPE). Proses enkripsi biasanya akan membuat ukuran header paket yang ditransmisikan akan bertambah.

Jika kita monitoring, traffick yang melewati tunnel PPTP akan mengalami overhead 7%.

2. L2TP (Layer 2 Tunnel Protocol)

L2TP merupakan pengembangan dari PPTP ditambah L2F. Network security Protocol dan enkripsi yang digunakan untuk autentikasi sama dengan PPTP. Akan tetapi untuk melakukan komunikasi, L2TP menggunakan UDP port 1701. Untuk keamanan yang lebih baik, L2TP dikombinasikan dengan IPSec, menjadi L2TP/IPSec. Contohnya untuk Operating system Windows, secara default OS Windows menggunakan L2TP/IPSec. Akan tetapi, konsekuensinya tentu saja konfigurasi yang harus dilakukan tidak se-simple PPTP. Sisi client pun harus sudah support IPSec ketika menerapkan L2TP/IPSec. Dari segi enkripsi, tentu enkripsi pada L2TP/IPSec memiliki tingkat sekuritas lebih tinggi daripada PPTP yg menggunakan MPPE. Traffic yang melewati tunnel L2TP akan mengalami overhead 12%.

3. SSTP (Secure Socket Tunneling Protocol)

Untuk membangun vpn dengan metode SSTP diperlukan sertifikat SSL di masing-masing perangkat, kecuali keduanya menggunakan RouterOS. Komunikasi SSTP menggunakan TCP port 443 (SSL), sama halnya seperti website yang secure (https). Anda harus memastikan *clock* sudah sesuai dengan waktu real jika menggunakan *certificate*. Menyamakan waktu router dengan real time bisa dengan fitur NTP Client. Belum semua OS Support VPN dengan metode SSTP. *Traffic* yang melewati tunnel SSTP akan mengalami overhead 12%.

4. OpenVPN

VPN ini Biasa digunakan ketika dibutuhkan keamanan data yg tinggi. Secara default, OpenVPN menggunakan UDP port 1194 dan dibutuhkan *certificate* pada masing-masing perangkat untuk bisa terkoneksi. Untuk client compatibility, OpenVPN bisa dibangun hampir pada semua Operating System dengan bantuan aplikasi pihak ketiga. OpenVPN menggunakan algoritma sha1 dan md5 untuk proses autentikasi, dan menggunakan beberapa chipper yaitu blowfish128, aes128, aes192 dan

aes256. Trafik yang melewati tunnel OpenVPN akan mengalami overhead 16%.

2.5. Enkripsi

Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti. Dengan enkripsi, berfungsi mengubah isi dari data yang kita kirim sehingga data tersebut tidak dapat dibaca oleh orang yang tidak berhak mendapatkannya. Informasi yang tidak diacak disebut clear-text sedangkan yang diacak disebut cipher-text. Di setiap tunnel VPN terdapat VPN gateway tempat pengiriman data mengenkripsi atau mengubah informasi clear-text menjadi cipher-text sebelum dikirim melalui tunnel ke internet. VPN gateway di tempat penerimaan mendeskripsikan atau mengubah cipher-text tersebut kembali menjadi clear-text.

Enkripsi terdiri dari dua jenis, yaitu symmetric encryption dan asymmetric encryption. Asymmetric encryption menggunakan public dan private key dalam proses enkripsi dan dekripsi, sedangkan symmetric encryption menggunakan key yang sama dalam proses enkripsi dan dekripsi.

Adapun metode encryption sebagai berikut:

1. Symmetric Encryption

Metode ini menggunakan private key berbagai komputer pengirim dan penerima sama-sama menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi informasi. Karena satu key digunakan bersama-sama untuk enkripsi dan dekripsi, maka harus ada pengertian antar kedua pihak untuk menjaga kerahasiaan key tersebut. Semua itu mempunyai kunci enkripsi dapat mendekripsi data yang terdapat dalam lalu lintas VPN. Jika ada user yang tidak berwenang memiliki kunci enkripsi, ia dapat mendekripsi data yang ada dan masuk kedalam jaringan yang

terhubung melalui VPN. Selain itu kunci enkripsi juga dapat dibuka dengan melakukan *brute force attack*. Hanya masalah waktu sampai seorang attacker dapat membuka kunci enkripsi.

2. Asymmetric Encryption

Asymmetric key encryption mengenkripsi informasi dengan satu key dan mendekripsi dengan key lainnya. Metode ini menggunakan kombinasi dari dua buah key, yaitu private key yang disimpan untuk diri sendiri, dan public key yang diberikan untuk remote-user. SSL menggunakan salah satu metode pengenkripsian asymmetric encryption ini untuk memastikan identifikasi dari masing-masing pengguna VPN.

2.6. Mikrotik

2.6.1 Pengertian Mikrotik

Mikrotik adalah sistem operasi berbasis Linux khusus untuk komputer yang difungsikan sebagai router. Mikrotik didesain untuk mudah digunakan dan sangat baik digunakan untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga yang kompleks. Mikrotik mulai didirikan tahun 1995 yang pada awalnya ditujukan untuk perusahaan jasa layanan Internet (Internet Service Provider, ISP) yang melayani pelanggannya menggunakan teknologi nirkabel.

Pada tahun 2002 Mikrotik membuat perangkat keras sendiri yang mempunyai kemampuan handal sebagai mesin router, yang akhirnya melahirkan merek RouterBoard. Mikrotik dikenal sebagai router yang irit hardware, mikrotik memiliki banyak fitur, mudah dikonfigurasi (*User Friendly*) dan dapat diinstall pada PC (*Personal Computer*) dan tersedia dalam bentuk dedicated router yang murah. Router Mikrotik dapat dikonfigurasi secara grafis maupun menggunakan perintah-perintah CLI (Command Line Interface). Mengkonfigurasi router mikrotik secara grafis dilakukan dengan

menggunakan aplikasi Winbox maupun melalui web browser. Mikrotik memiliki banyak peran dalam jaringan komputer karena mikrotik memiliki banyak fitur yang dapat digunakan dalam merancang dan membangun suatu jaringan komputer. Saat ini MikroTik memberikan layanan kepada banyak ISP nirkabel untuk layanan akses Internet di banyak negara di dunia dan juga sangat populer di Indonesia.

Mikrotik RouterBoard merupakan hardware (router) yang didesain oleh Mikrotik yang memiliki beragam seri dan interface yang disesuaikan dengan kebutuhan. RouterBoard sendiri menggunakan RouterOS sebagai software / sistem operasinya. Mikrotik pada standar perangkat keras berbasis *Personal Computer* (PC) dikenal dengan kestabilan, kualitas kontrol dan fleksibilitas untuk berbagai jenis paket data dan penanganan proses rute (routing). Mikrotik yang dibuat sebagai router berbasis komputer banyak bermanfaat untuk sebuah ISP yang ingin menjalankan beberapa aplikasi mulai dari hal yang paling ringan hingga tingkat lanjut. Beberapa contoh RouterBoard dari Mikrotik diantaranya adalah RB400, RB600, R52H, R52N, R2N, RB750, RB450G, RB951U, RB1000. Dan penulis sendiri menggunakan RB941-2nd TC sebagai router untuk menunjang dalam implementasi. Selain routing, Mikrotik dapat digunakan sebagai manajemen kapasitas akses (bandwidth, firewall, wireless access point (WiFi), backhaul link, system hotspot, Virtual Private Network server dan masih banyak lainnya.

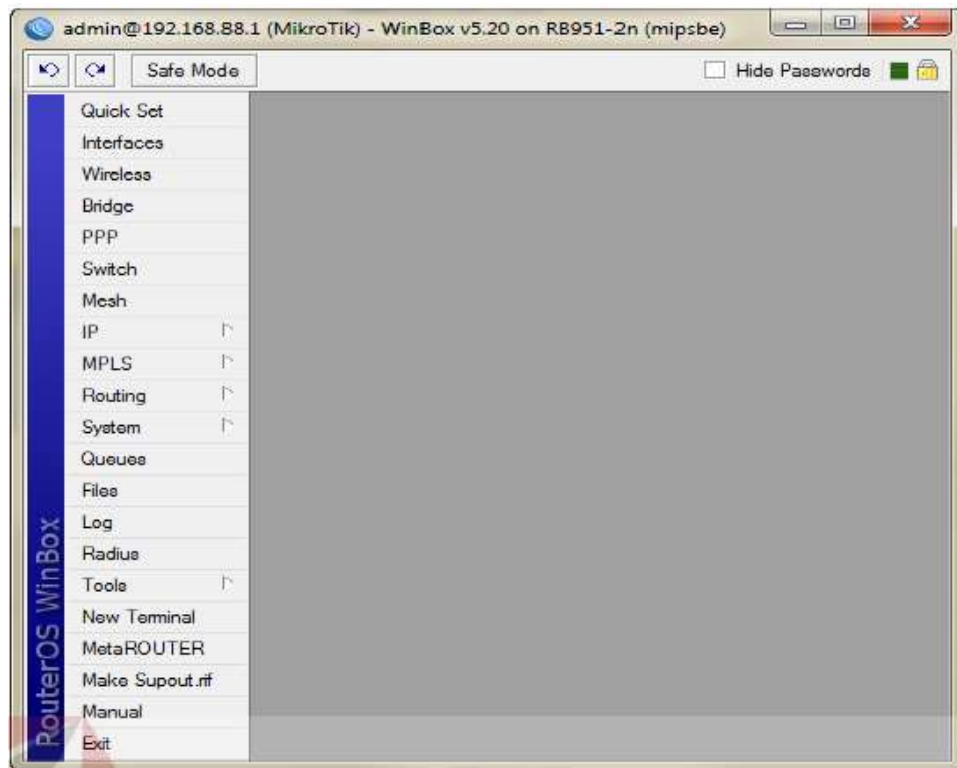


Gambar 2. 14 Mikrotik RB-941 2nd TC

Mikrotik bukanlah perangkat lunak yang gratis jika ingin memanfaatkannya secara penuh, dibutuhkan lisensi dari MikroTik untuk dapat menggunakannya dengan cara membayar. Mikrotik dikenal dengan istilah Level pada lisensinya.

1. Level 0 (gratis), tidak membutuhkan lisensi untuk menggunakannya dan penggunaan fitur hanya dibatasi selama 24 jam setelah instalasi dilakukan.
2. Level 1 (demo), pada level ini kamu dapat menggunakannya sbg fungsi routing standar saja dengan 1 pengaturan serta tidak memiliki limitasi waktu untuk menggunakannya.
3. Level 3, sudah mencakup level 1 ditambah dengan kemampuan untuk manajemen segala perangkat keras yang berbasiskan Kartu Jaringan atau Ethernet dan pengelolaan perangkat wireless tipe client.
4. Level 4, sudah mencakup level 1 dan 3 ditambah dengan kemampuan untuk mengelola perangkat wireless tipe access point.
5. Level 5, mencakup level 1, 3 dan 4 ditambah dengan kemampuan mengelola jumlah pengguna hotspot yang lebih banyak.

6. Level 6, mencakup semua level dan tidak memiliki limitasi atau Batasan apapun.



Gambar 2. 15 Tampilan utama Winbox

2.6.2 Fitur Mikrotik

Mikrotik mempunyai banyak fitur yang disediakan. Karena begitu banyaknya penulis hanya menjelaskan beberapa fungsi penting yang terdapat pada Router Mikrotik. Berikut ini adalah beberapa fitur yang terdapat pada Mikrotik Router :

1. Address List

Merupakan kumpulan kelompok IP Address yang berdasarkan nama

2. Bridge

Berfungsi untuk menghubungkan beberapa network menjadi satu segmen network yang sama

3. Data Rate Management

Mendukung QOS (Quality of Service) yang digunakan untuk melakukan management bandwidth

4. Asynchronous

Dukungan untuk serial PPP dial-in atau dial-out, memiliki otentikasi CHAP, PAP, MSCHAPv1 dan MSCHAPv2, Radius, dial on demand, modem pool hingga 128 ports.

5. Bonding

Penggabungan beberapa interface menjadi sebuah virtual link, ditujukan untuk peningkatan data rate

6. DHCP

Mendukung DHCP Service seperti DHCP Server, DHCP Client, DHCP Relay.

7. NTP (Network Time Protocol)

Mendukung sinkronasi waktu dengan waktu di seluruh dunia.

8. Point to Point Tunneling Protocol

Mendukung untuk membuat jaringan berbasis virtual private network dengan metode tunneling.

9. Proxy

Kemampuannya untuk Cache FTP dan HTTP proxy server, HTTP proxy bisa juga untuk transparent proxy DNS dan HTTP serta mendukung protokol SOCKS, parent proxy, static DNS

10. Routing

Mendukung protokol routing seperti RIP, OSPF, BGP, dll

11. Firewall

Digunakan untuk melakukan filterisasi content terhadap lalu lintas data dalam jaringan.

12. Hotspot

Memungkinkan untuk membuat hotspot gateway dengan otentikasi radius server.

13. Tools

Memiliki beberapa tools yang digunakan dalam jaringan

14. VLAN

Mendukung Virtual LAN untuk interface ethernet dan wireless

BAB III

METODE PENELITIAN

Metodologi penelitian ini dilakukan menggunakan metode analisis terhadap kinerja suatu jaringan VPN pada MikroTik router. Metode ini lebih berkaitan dengan kinerja yang didasarkan oleh beberapa variabel dan parameter. MikroTik digunakan sebagai peralatan utama dalam proses penelitian ini.

3.1. Penelitian Terkait

3.1.1 Hendra Supendar (2016)

Penelitian ini disusun berdasarkan beberapa penelitian sebelumnya, diantaranya dari penelitian yang Berjudul Analisis Perbandingan Kinerja Jaringan VPN Berbasis Mikrotik Menggunakan Protokol Point to Point Tunneling Protokol (PPTP) Dan Layer 2 Tunneling Protocol (L2TP) Sebagai Media Transfer Data. Dalam laporan penelitiannya VPN dibangun agar Penggunaan jaringan VPN dapat memberikan sebuah alternatif untuk melakukan akses pada sebuah situs web yang berdekatan dengan dengan jaringan VPN itu sendiri.

Kemudian penelitian tentang VPN-PPTP yang berjudul Perbandingan Performansi Jaringan Virtual Private Network Metode Point To Point Tunneling Protocol (PPTP). Tujuan penelitian ini untuk untuk membandingkan performansi tunneling jaringan Virtual Private Network metode Point to Point Tunneling Protocol (PPTP) dan metode Internet Protocol Security (IPsec) yang dapat membantu para pakar jaringan untuk menyesuaikan tunneling mana yang sesuai dengan kondisi lapangan karena dengan penelitian ini dapat terlihat perbandingan performansi dari sisi waktu transmisi, delay, bandwidth, jitter serta troughput saat proses transmisi data.

Metodologi penelitian ini dilakukan menggunakan metode analisis terhadap kinerja suatu jaringan awal dimana permasalahan yang dihadapi saat ini adalah jaringan yang berada dalam satu area selain berhubungan dan berkomunikasi dengan menggunakan flash disk atau sharing file.

Sementara untuk berhubungan antara kantor dengan kantor menggunakan internet dan email untuk mengirim data dan berkomunikasi. Hal ini menyebabkan keamanan data yang dikirim tidak bisa dijamin. Merancang dan mengimplementasikan virtual private network (VPN) menggunakan mikrotik secara remote site merupakan salah satu solusi alternatif dimana dapat membantu komunikasi atau transfer data antar-cabang secara aman melalui jalur koneksi internet seperti seolah-olah melalui jaringan lokal. Dengan merancang VPN ini diharapkan dapat memberi keamanan dan kemudahan proses transfer data dan komunikasi antar-cabang. Setelah di implementasikan maka jaringan VPN tersebut di teliti kembali untuk menguji kehandalannya. Metode ini lebih berkaitan dengan kinerja yang didasarkan oleh beberapa variabel dan parameter MikroTik digunakan sebagai peralatan utama dalam proses penelitian tersebut. Pada evaluasi keamanan jaringan terbukti bahwa menggunakan VPN dengan protokol PPTP terdapat kompres data, enkapsulasi dan enkripsi.

3.1.2 E. Mufida, D. Irawan dan G. Chrisnawati (2017)

Penelitian ini dilakukan di Yayasan Teratai Putih yang memiliki 9 (Sembilan) unit sekolah mulai dari PG/TK, SD Islam, SMP Islam, SMA Islam serta SMK yang tersebar di Bekasi dan Jakarta. Dalam proses pendataan terutama berkaitan dengan keuangan siswa, kesembilan unit tersebut memiliki perangkat lunak sistem administrasi sekolah pada unit sekolah masing-masing, kondisi ini menyulitkan pihak yayasan dalam proses konsolidasi data. Proses pengambilan data yang masih manual dengan datang ke lokasi masing-masing sekolah, karena bila data dikirim via email, selain kurang aman juga terkendala batasan kapasitas ukuran file yang dikirim dalam sekali pengiriman menggunakan email.

Dengan memanfaatkan internet, Selain mudah dan cepat, penggunaan internet dapat menekan biaya operasional perusahaan. Tetapi, dengan segala kelebihanannya, internet juga memiliki kelemahan. Internet yang dapat diakses oleh semua orang membuatnya menjadi tidak

aman untuk mengirimkan informasi yang sifatnya rahasia. Apalagi sudah banyak bermunculan aplikasi-aplikasi yang bisa membobol pesan dengan sangat mudah, yang dilakukan oleh para hacker yang tidak bertanggung jawab. Oleh karena itu, penggunaan internet di dalam perusahaan juga harus disertai dengan penggunaan sistem keamanan yang terpercaya. Saat ini, Internet juga dapat digunakan untuk menghubungkan jaringan intranet kantor pusat, yaitu sebuah jaringan internal yang berada di dalam perusahaan, dengan 1 atau 2 jaringan intranet di kantor cabang. Teknologi jaringan yang dapat mendukung hal ini adalah teknologi VPN, yaitu teknik yang dapat menghubungkan beberapa jaringan local melalui jaringan publik (internet) dengan teknik VPN komunikasi seakan-akan kedua jaringan tersebut berada di dalam satu jaringan intranet yang besar.

Pada skema jaringan di SMK Teratai Putih 2, SMK Teratai Putih 3 dan jaringan kantor yayasan teratai putih. terdapat jaringan yang terpisah antara sekolah dan yayasan, masing-masing memiliki koneksi internet dengan ISP yang berbeda. pada yayasan teratai putih menggunakan jasa ISP central Online serta terdapat switch yang mengakomodir jaringan LAN pada masing-masing lokasi. Dan Pada tiap-tiap sekolah terdapat satu modem, satu switch serta PC dengan koneksi internet menggunakan Indihome, semua itu terhubung ke internet.

Yayasan memiliki satu buah IP Public static. Semua IP komputer staff dan karyawan menggunakan konfigurasi IP secara manual. Semua terkoneksi ke router melalui hub/switch dan terkoneksi ke internet. Server pada yayasan masih menggunakan windows XP yang di dalamnya berjalan aplikasi Excellent (aplikasi mengatur keuangan sekolah). Dari komputer server, semua komputer client yang berada di yayasan dapat mengakses data base Excellent sehingga dapat dipergunakan untuk transaksi. Sedangkan setiap sekolah hanya bisa menginput data murid, kemudian diberikan ke kantor yayasan untuk di input melalui aplikasi Excellent. Setiap jaringan tidak pernah lepas dari serangan, serangan bisa terjadi kapanpun, yang akan berdampak pada kestabilan dan produktifitas jaringan, Keamanan jaringan yang sedang digunakan pada yayasan

teratai putih hanya menggunakan default bawaan perangkat jaringan komputer yang digunakan tanpa ada tambahan, pengamanan instalasi standard mode pengamanan biasa seperti firewall default dari router, password security WPA2/PSK serta user login password yang sangat mudah diretas. Selain itu, Semua perangkat komputer yang digunakan bisa dengan bebas menggunakan koneksi internet, tanpa ada proxy yang diaktifkan untuk menyaring dan memblokir sebuah situs yang tidak layak. Selain itu, koneksi antar sekolah juga menggunakan akses langsung, sehingga dapat menimbulkan celah pihak eksternal masuk ke jaringan internal di Yayasan Teratai Putih Global. Secara garis besar permasalahan yang dihadapi oleh Yayasan Teratai Putih Global yaitu dalam penarikan data transaksi kantor pusat ke sekolah-sekolah yang bersifat sangat rahasia. Dari permasalahan tersebut, Jaringan usulan yang akan diterapkan adalah membangun sebuah sistem jaringan VPN dengan menggunakan router Mikrotik, merupakan suatu sistem keamanan yang digunakan untuk mengamankan jaringan komunikasi yang menghubungkan yayasan dengan sekolah-sekolah yang bernaung di bawah Yayasan Teratai Putih Global. Jaringan yang terhubung dan dibentuk dari VPN merupakan suatu pipa (tunnel) yang berada di jaringan publik sehingga aliran data yang melewati di dalamnya tidak bisa diakses oleh pihak lain yang tidak memiliki akses ke dalam tunnel tersebut.

3.1.3 Fitri Sjafrina, Pipit Dewi Arnesia dan Arif Aqim (2019)

Penelitian ini menggunakan dua metode, yaitu Pengumpulan data dan Pengembangan Sistem.

a. Metode Pengumpulan Data

Penelitian kualitatif berakar pada latar alamiah sebagai keutuhan, dan mengadakan analisis data secara induktif yang mengarahkan sasaran penelitiannya pada usaha menemukan teori dari dasar yang bersifat deskriptif. Proses dalam penelitian kualitatif lebih dipentingkan daripada hasil, dan hasil penelitiannya disepakati oleh kedua belah pihak yaitu peneliti dan subjek penelitian.

b. Metode Pengembangan Sistem

Metode yang digunakan dalam melakukan rancang bangun dan pengembangan sistem yaitu menggunakan Network Development Life Cycle (NDLC). Metode ini memiliki enam tahapan, yaitu tahap analysis, design, simulation prototyping, implementation, monitoring, dan management, seperti pada gambar Model pengembangan sistem NDLC dimulai pada fase analisis dimana pada tahap ini membahas proses analisis pembangunan VPN sistem dan perancangan VPN sistem. Sebelum dilakukan pengembangan dan perancangan sistem, terlebih dahulu dilaksanakan analisis kebutuhan-kebutuhan pokok Jaringan VPN yang akan dibangun.

Dalam penelitian ini terdapat kesimpulan bahwa Kantor pusat dan cabang dapat terhubung ke jaringan VPN dengan konektivitas bandwidth internet yang high speed internet residential package dari Internet Service provider memiliki kecepatan up to 100 Mbps. VPN berbasis IPSec dapat diimplementasikan pada Mikrotik Routerboard dengan konfigurasi Mikrotik IP Address, DHCP Client, DNS Server, Masquarade Firewall, Hotspot dan Security Firewall, dimana hasil dari tahapan sebelumnya melalui proses implementasi yang dilakukan adalah instalasi dan konfigurasi menggunakan routerboard dengan mikrotik yang sudah diinstalasi di dalam routerboard. Selanjutnya memonitor aktifitas pengoperasian dan pengamatan uji coba koneksi jaringan dengan cara koneksi akses remote VPN yang sudah dibangun menggunakan sambungan sederhana yang terdaftar di VPN server, kemudian klik Connect; setelah proses Authentication sukses, maka VPN sudah terkoneksi dengan jaringan.

Dalam penelitian ini diambil kesimpulan bahwa dengan menggunakan VPN dapat mempermudah dan efisiensi waktu dalam pertukaran data hanya dengan mengaktifkan VPN client. VPN dengan protokol PPTP terbukti memberikan keamanan pada data dan konektivitas jaringan. Hal ini ditunjukkan pada saat VPN client melakukan log in ke VPN server akan terdapat autentikasi username dan password, terdapat juga enkapsulasi dan enkripsi data serta integritas data yang telah terbukti

pada simulasinya. VPN rentan terhadap serangan Denial of Service (DoS) atau serangan lainnya namun dapat ditangani dengan memblokir protokol ICMP sehingga IP public tidak dapat di ping. Dengan membandingkan jaringan yang berjalan dengan VPN dan dengan jaringan yang menggunakan modem 3G maka ternyata jaringan yang menggunakan VPN walaupun mempunyai packet loss yang lebih banyak namun mempunyai round trip yang lebih baik serta memiliki transfer data yang lebih cepat. Pada evaluasi keamanan jaringan terbukti bahwa menggunakan VPN dengan protokol PPTP terdapat kompres data, enkapsulasi dan enkripsi.

3.1.4 Puputro Sanzoyo Utomo (2020)

Pada Penelitian ini bertujuan untuk menganalisa pengaruh data kompresi-dekompresi, enkripsi-dekripsi dan kombinasi serta menggunakan aplikasi kompresi dengan membedakan format data, ukuran data yang diatur bandwidth sehingga akan diketahui transfer rate di jaringan VPN tersebut.

Dalam jaringan komputer, faktor keamanan menjadi penting terutama bila digunakan jaringan public. VPN merupakan solusi tepat untuk koneksi antar cabang di suatu organisasi. Berdasarkan hal tersebut didapat permasalahan tentang bagaimana karakteristik transfer pada kondisi enkripsi-dekripsi dan kompresi-dekompresi.

Lingkup permasalahan penelitian ini adalah sebagai berikut:

1. Menentukan performa transfer rate dan diatur berdasarkan format data, ukuran data, kompresi-dekompresi, enkripsi-dekripsi.
2. Perancangan model (design) jaringan VPN menggunakan aplikasi VPN mikrotik dan Open VPN.
3. Pengujian yang dilakukan pada sisi Client akan menggunakan dua OS (Operating System), yaitu Windows XP
3. Analisis terhadap hasil yang diperoleh dilakukan dengan menggunakan simulator winbox kemudian dibandingkan hasilnya.
4. Tidak membahas keamanan yang lebih detail.

3.2. Permasalahan Sistem Jaringan

Permasalahan sistem jaringan komputer pada SMK Islam Manbaul Hikmah Luwunragi, yaitu:

1. Belum menerapkan sistem keamanan untuk saling tukar data antara kantor SMK dan di rumah masing masing.
2. Sinyal wifi yang lemah sehingga karyawan yang menggunakan laptop tidak bisa terkoneksi dengan baik.
3. Kendala dalam pengiriman email antara kantor SMK dan rumah, jika terdapat data dengan ukuran besar. Tanpa menanggung biaya yang besar dan agar lebih aman karena menggunakan metode enkripsi.

3.3. Analisa Penelitian

Pada penelitian ini dilakukan analisa sebagai berikut :

1. Meliputi pengumpulan, penyeleksian, pengolahan, data yang berhubungan dengan jaringan VPN. Pada tahap ini proses dilakukan penentuan variabel data test, yaitu data apa saja yang akan di jadikan pembanding untuk menganalisis kinerja yang terjadi pada jaringan VPN.
2. Penjelasan mengenai variabel-variabel, bagaimana cara menentukan kinerja berdasarkan hasil pengukuran terhadap variabel-variabel tersebut.
3. Jaringan VPN ini dibangun menggunakan protocol TCP/IP sebagai protocol untuk melakukan komunikasi data antar komputer, dan melakukan fungsi komunikasi pada internet. Jaringan VPN ini menggunakan mikrotik sebagai router dan proses tunneling dengan VPN PPTP. PPTP digunakan untuk mengamankan koneksi PPP melewati jaringan TCP/IP
4. Untuk melihat kinerja VPN menggunakan mikrotik, maka diperlukan pembanding dengan penerapan VPN yang lain Dalam hal ini penulis melakukan percobaan VPN berbasis software open source yaitu dengan Open VPN. Dengan membandingkan penerapan antara 2 implementasi VPN pada kondisi yang sama (Hardware & Software),

diharapkan di peroleh hasil perbandingan kinerja yang akurat yang dapat dipercaya akan di rancang Virtual Private Network (VPN) dengan menggunakan metode PPTP, MikroTik digunakan sebagai Router dalam penelitian ini.

3.2.1 Alat dan Kebutuhan Bahan

Adapun alat dan bahan yang akan digunakan dalam penelitian ini dapat dibedakan dalam dua kategori yaitu hardware (perangkat keras) dan software (perangkat lunak).

1. Perangkat Keras (Hardware)

No	Hardware	
	Nama	Spesifikasi
1.	Laptop / PC	Merk : Asus A50C, Processor : Intel Core i5-3337U 1.80 GHz, Memori : 6 GB Harddisk : 320 GB
2.	Routerboard	Mikrotik 941-2nd TC

Tabel 3. 1 Kebutuhan Perangkat Keras

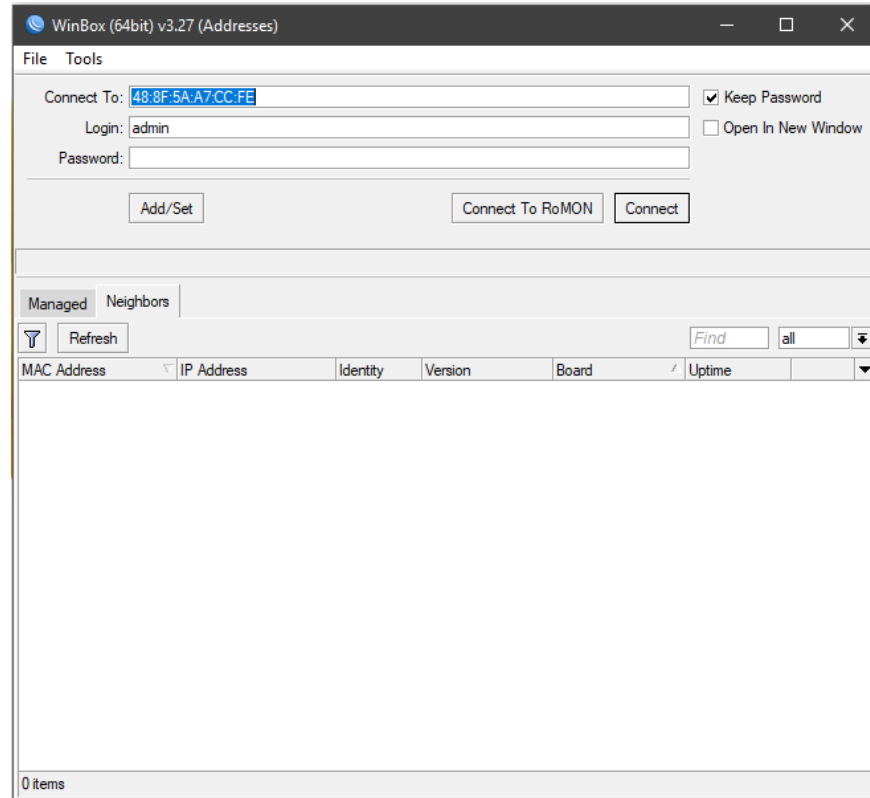
2. Perangkat Lunak (Software)

a. Windows 10.

Untuk membangun jaringan hotspot digunakan operasi system windows 10.

b. Winbox

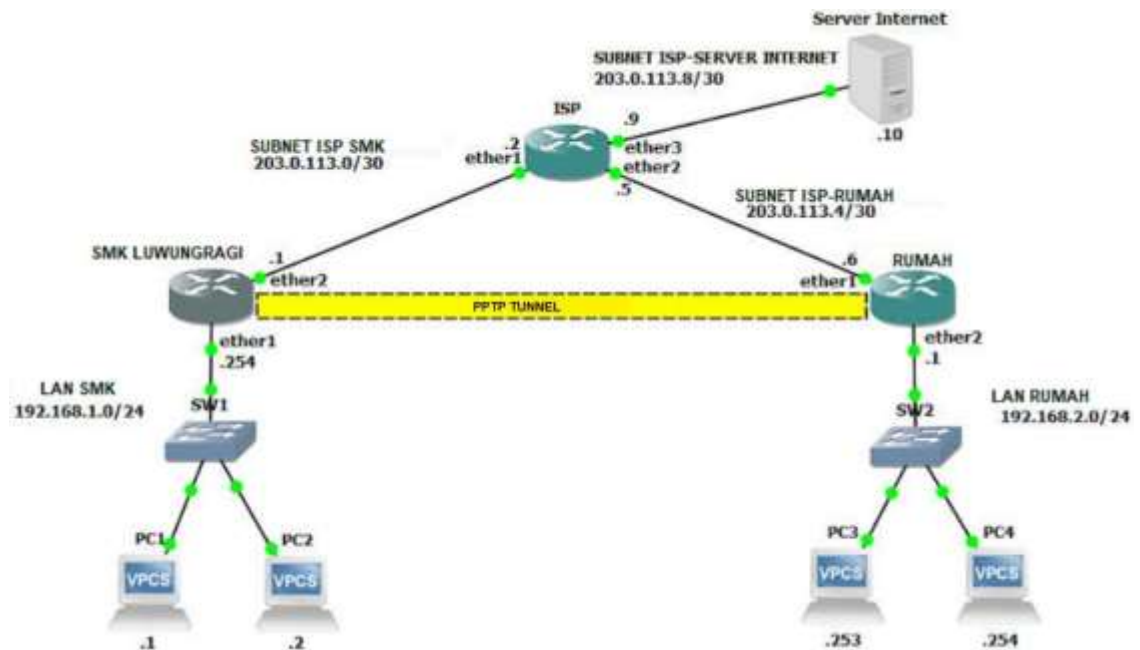
Winbox merupakan sebuah remote yang dikeluarkan oleh mikrotik untuk dapat dilakukan konfigurasi pada mikrotik. Dalam penelitian ini menggunakan winbox versi 3.27



Gambar 3. 1 Tampilan Aplikasi Winbox

3.2.2 Desain

Dari data yang didapatkan sebelumnya, tahap design ini akan membuat gambar desain topologi jaringan interkoneksi yang akan dibangun. Diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada. Desain bisa berupa desain struktur topologi, desain akses data, desain layout perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang proyek yang akan dibangun. Biasanya hasil dari design berupa: Gambar gambar topologi (server farm, firewall, datacenter, storages, lastmiles, perkabelan, titik akses dan sebagainya); Gambar-gambar detail estimasi kebutuhan yang ada. Dan dalam desain juga menggambarkan topologi dan skema jaringan yang akan di bangun dengan teknologi VPN yang disimulasikan menggunakan virtual box.



Gambar 3. 2 Desain Topologi Jaringan VPN

3.2.3 Pengujian

Tahap pengujian jaringan komputer yang telah dibuat akan dilakukan uji coba untuk mengetahui kelebihan dan kekurangan pada jaringan komputer yang telah dipasang. Beberapa pekerja jaringan akan membuat dalam bentuk simulasi dengan bantuan tools khusus di bidang network seperti Cisco Packet Tracer, Netsim, dan sebagainya. Hal ini dimaksudkan untuk melihat kinerja awal dari jaringan yang akan dibangun dan sebagai bahan presentasi dan sharing dengan team work lainnya.



Gambar 3. 3 Transfer Rate VPN

3.4. Metode Pengumpulan Data

Metode pengumpulan data yang dilakukan pada penelitian ini adalah:

3.3.1 Observasi

Observasi dilakukan dengan cara peninjauan ke lokasi untuk tujuan mengetahui keadaan jaringan dan mengumpulkan data dan informasi yang nantinya akan digunakan untuk pengembangan jaringan di SMK Islam Manbaul Hikmah Luwungragi.

3.3.2 Wawancara

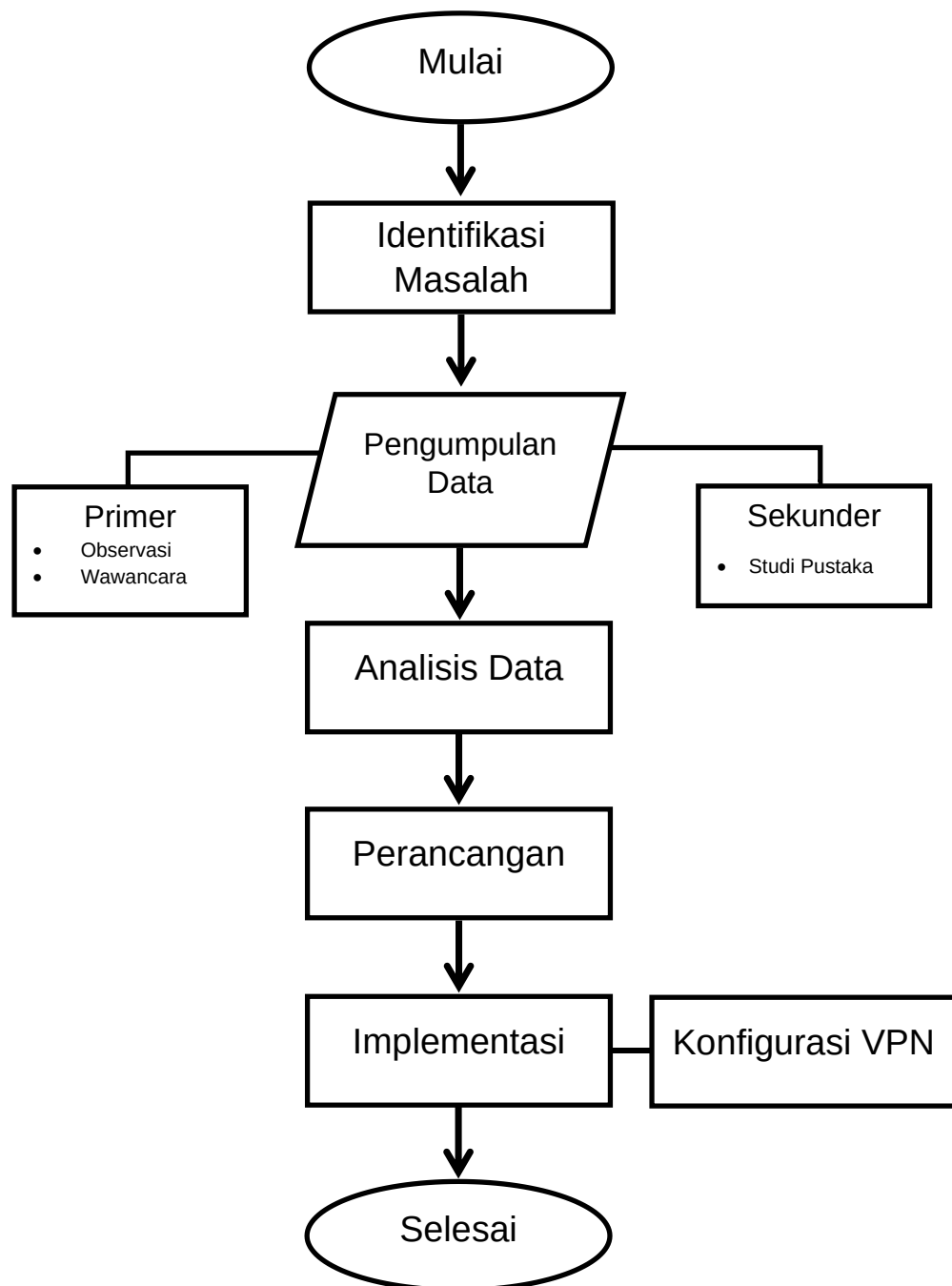
Wawancara dilakukan dengan Tanya jawab secara langsung mengenai jaringan yang ada di SMK Islam Manbaul Hikmah Luwungragi dengan seorang teknisi bagian IT. Wawancara dilakukan dengan pihak terkait melibatkan dari struktur manajemen atas sampai ke level bawah/ operator agar mendapatkan data yang konkrit dan lengkap. Pada kasus di *Computer Engineering* biasanya juga melakukan *brainstorming* juga dari pihak vendor untuk solusi yang ditawarkan dari vendor tersebut karena setiap mempunyai karakteristik yang berbeda; Survey langsung kelapangan, pada tahap analisis juga biasanya dilakukan survey langsung kelapangan untuk mendapatkan hasil sesungguhnya dan gambaran

seutuhnya sebelum masuk ke tahap desain. Survey biasa dilengkapi dengan alat ukur seperti GPS dan alat lain sesuai kebutuhan untuk mengetahui detail yang dilakukan; Membaca buku manual, pada analisis awal ini juga dilakukan dengan mencari informasi dari buku manual dokumentasi yang mungkin pernah dibuat sebelumnya. Sudah menjadi keharusan dalam setiap pengembangan suatu sistem dokumentasi menjadi pendukung akhir dari pengembangan tersebut. Begitu juga pada proyek jaringan, dokumentasi menjadi syarat mutlak setelah sistem selesai dibangun.

3.3.3 Studi Pustaka

Pencarian referensi dan sumber yang berhubungan dengan VPN, PPTP dan simulasinya, pencarian referensi atau sumber yang berhubungan dengan MikroTik. Mempelajari dan memahami proses konfigurasi VPN pada MikroTik. Referensi didapat dari jurnal atau buku. Pengumpulan bahan-bahan pustaka baik yang dilakukan di perpustakaan maupun melalui pencarian lewat internet yang dapat membantu memperdalam materi, pembuatan rancangan jaringan dan pengujian sistem jaringan yang dibuat.

3.5. Kerangka Berpikir



Gambar 3.4. Kerangka Berpikir

Proses Penelitian dibuat mulai dari Pengumpulan Data. Dalam langkah ini peneliti melakukan pengumpulan data melalui wawancara.

Peneliti melakukan wawancara dengan salah satu pegawai instansi yang berkompeten di bidang komputer dan jaringan, yaitu Bapak Muhamad Aslah, S.Ds, MTCNA, MTCRE.

Selanjutnya peneliti melakukan Observasi. Peneliti melakukan survey langsung ke lapangan, dengan didampingi oleh Bapak Muhamad Aslah, S.Ds, MTCNA, MTCRE. Beliau menjelaskan instalasi jaringan yang ada di SMK Islam Manbaul Hikmah Luwungragi.

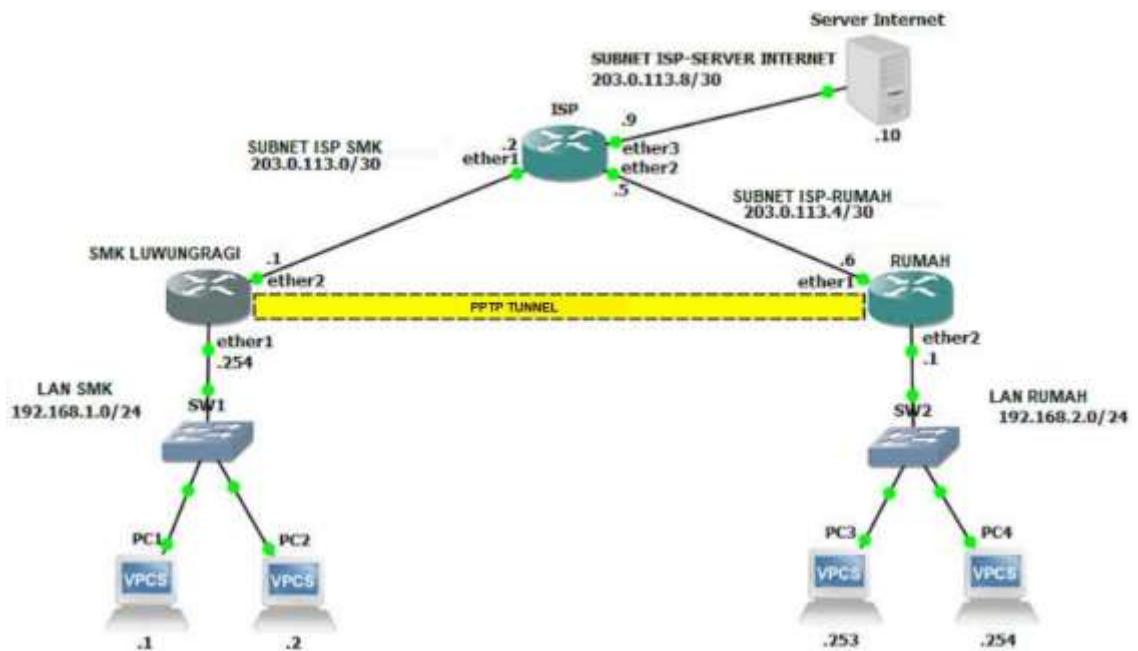
Studi pustaka dilakukan dengan membaca beberapa buku, jurnal, dan beberapa sumber data dari internet. Kemudian mengidentifikasi masalah yang terjadi di SMK Islam Manbaul Hikmah Luwungragi. Kemudian mengetahui masalah yang ada di SMK Islam Manbaul Hikmah Luwungragi, lalu menetapkan tujuan dan manfaat untuk penelitian ini.

Setelah data diperoleh, selanjutnya mengelolah data yang telah dikumpulkan. Data tersebut diidentifikasi faktor penyebabnya dan masalah apa yang muncul.

Kemudian menganalisis data yang sudah diolah supaya dapat mengajukan usulan pemecahan masalah. Kemudian melakukan perancangan dan implementasi berupa konfigurasi VPN untuk membuat kesimpulan.

BAB IV IMPLEMENTASI SISTEM

4.1 Simulasi Topologi Jaringan

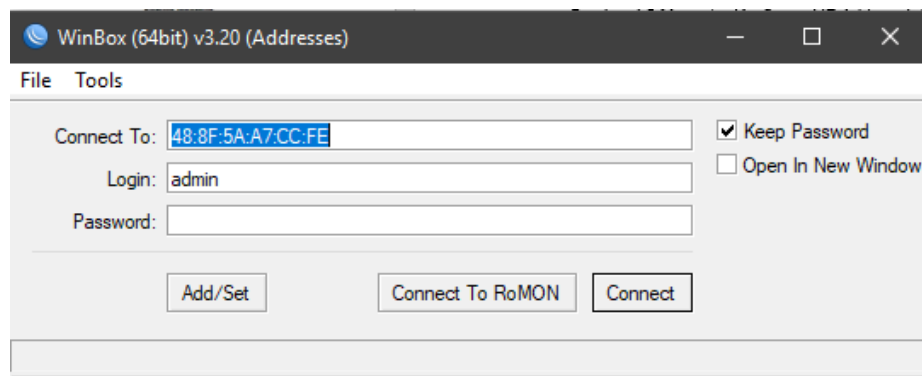


Gambar 4. 1 Desain Topologi Jaringan VPN

4.2 Konfigurasi Mikrotik

a. Login Mikrotik

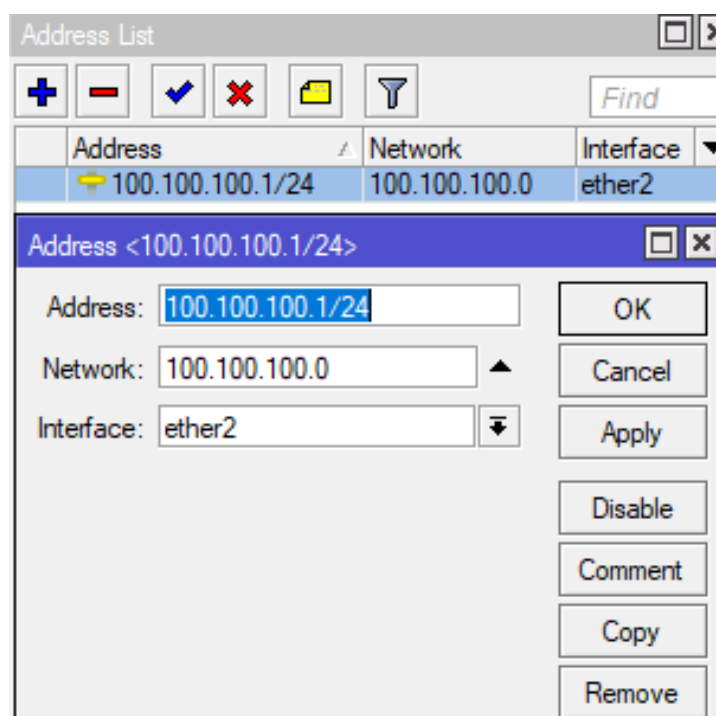
Open aplikasi winbox dan pada kolom Connect to Pilih Mac Address Mikrotik yang akan digunakan. Untuk login menggunakan user dan password default.



Gambar 4. 2 Menjalankan aplikasi Winbox

b. Pengaturan IP Address pada Mikrotik Router Kantor SMK

Pada router ini penulis menggunakan 2 ether, ether 1 untuk IP Public dan ether 2 untuk IP Local. Langkah memberikan IP Address pada masing – masing interface dengan klik Menu | IP | Address | pada tampilan Address List klik tombol + warna merah.

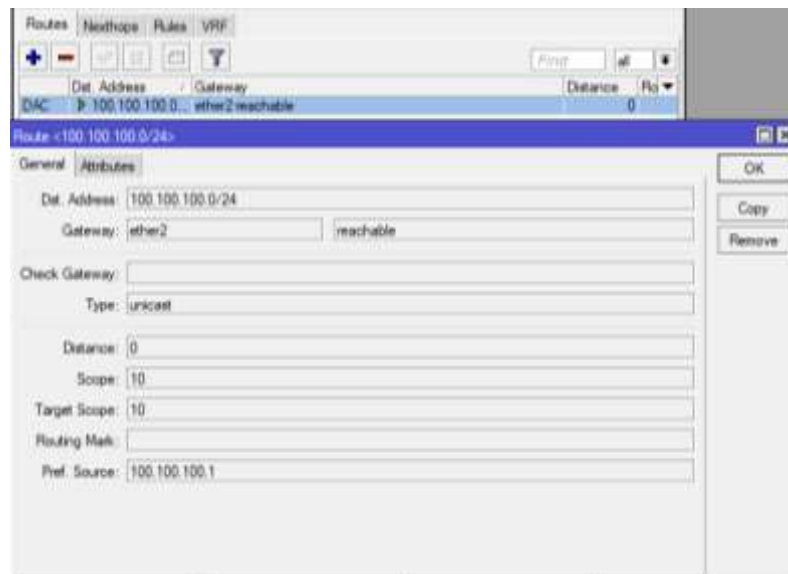


Gambar 4. 3 Pengaturan IP Address

c. Pengaturan Route Table

Set Route pada Mikrotik Router bertujuan untuk menentukan jalur gateway dari jaringan lokal ke jaringan yang terkoneksi internet. Dengan

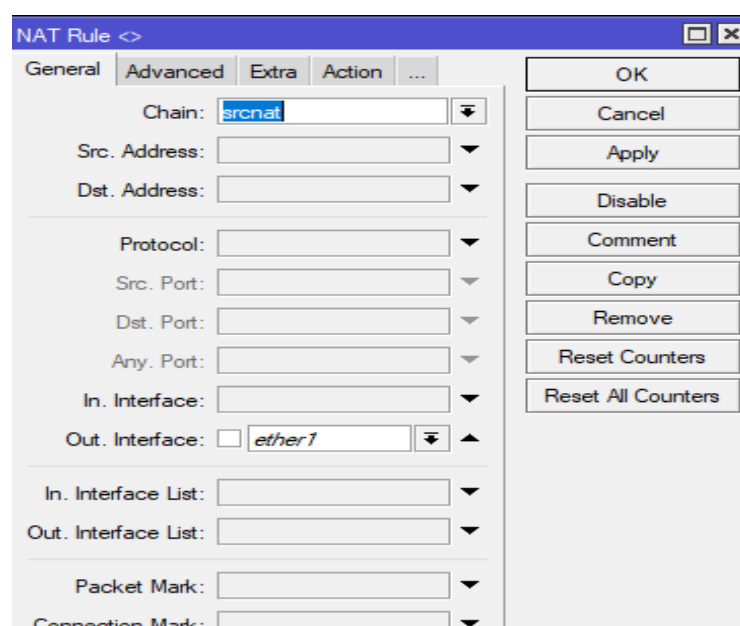
cara klik Menu IP| Routes| pada tampilan Route List klik tombol + warna merah untuk menambahkan gateway

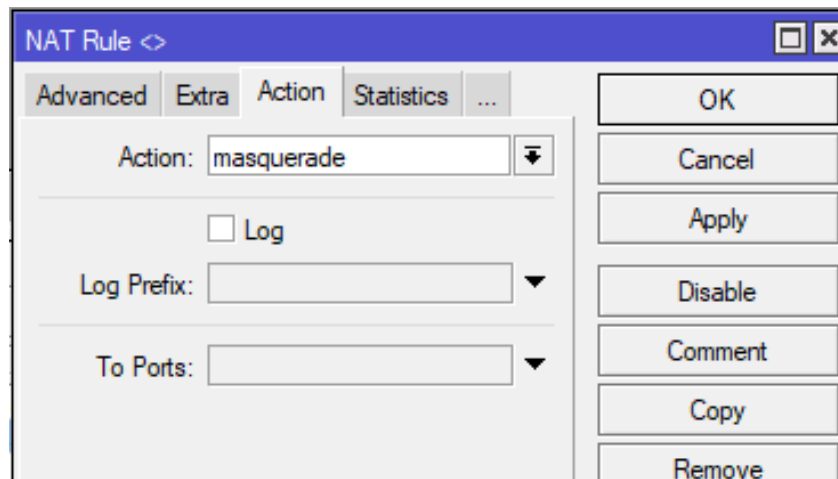


Gambar 4. 4 Pengaturan Route Table

d. Pengaturan Firewall NAT

Network Address Translation (NAT) adalah suatu metode menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP. Klik Menu IP| Firewall | NAT. Setting seperti gambar:

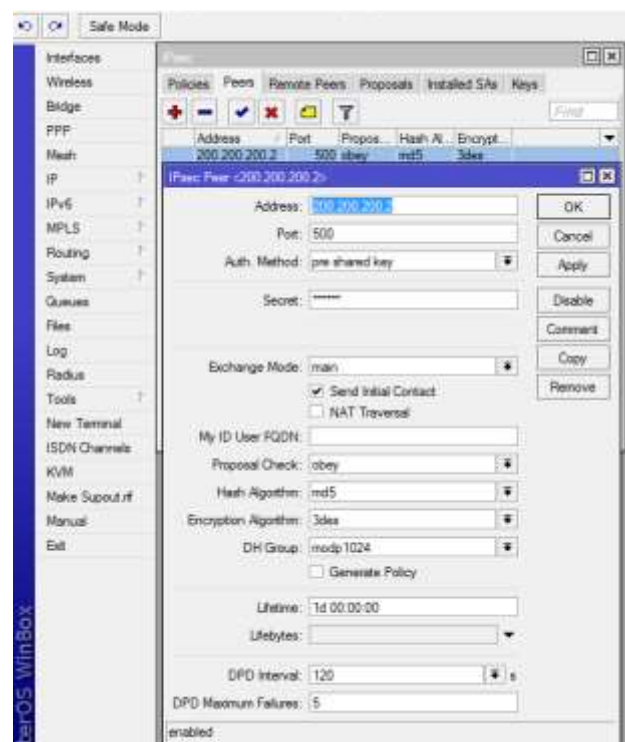




Gambar 4. 5 Pengaturan Nat

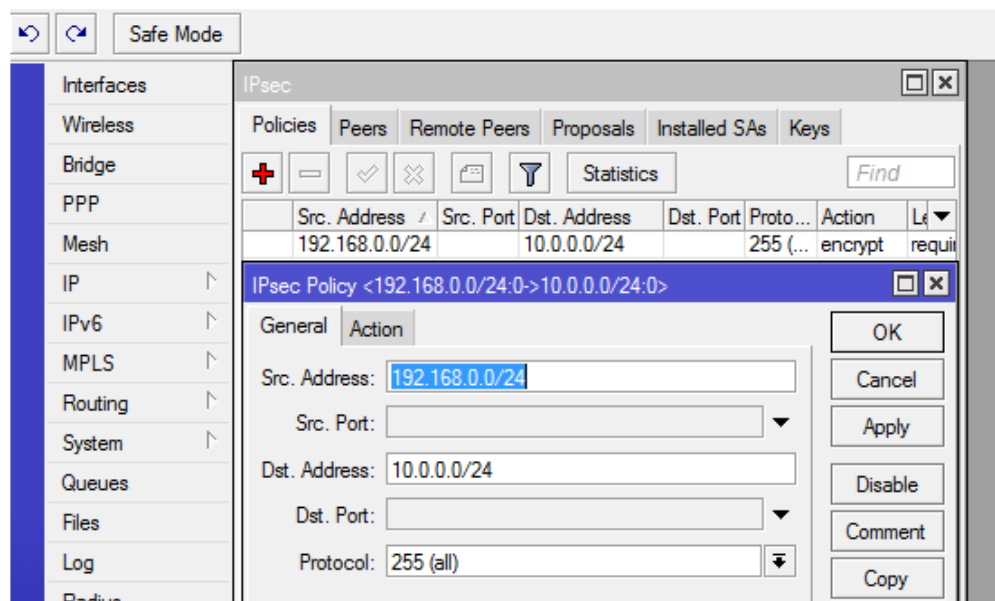
e. Pengaturan IPSec Peer

IPSec adalah sebuah protokol yang digunakan untuk mengamankan transmisi datagram dalam sebuah internetwork berbasis TCP/IP. Klik Menu IP|IPSec|Peers. Setting seperti gambar :



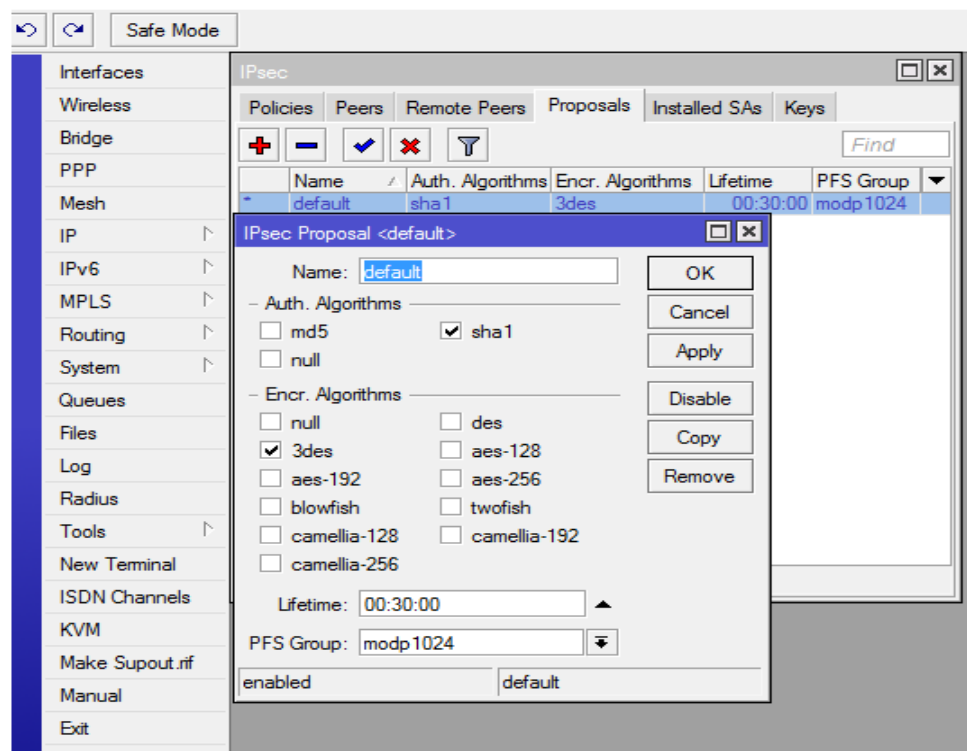
Gambar 4. 6 Pengaturan IPSec Peer

Selanjutnya setting pada Tab IPsec Policy, tambahkan juga parameter pada tampilan berikut :



Gambar 4. 7 Pengaturan IPsec Policy

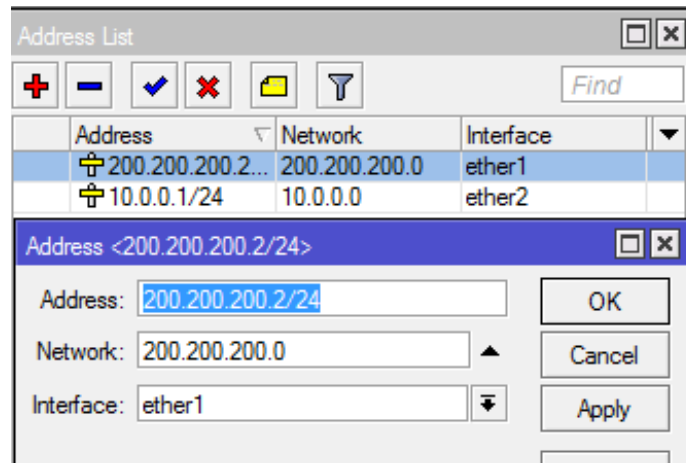
Selanjutnya setting pada Tab IPsec|Proposal |, tambahkan juga parameter pada tampilan berikut :



Gambar 4. 8 Pengaturan IPsec Proposal

8. Pengaturan IP Address pada Mikrotik Router Rumah

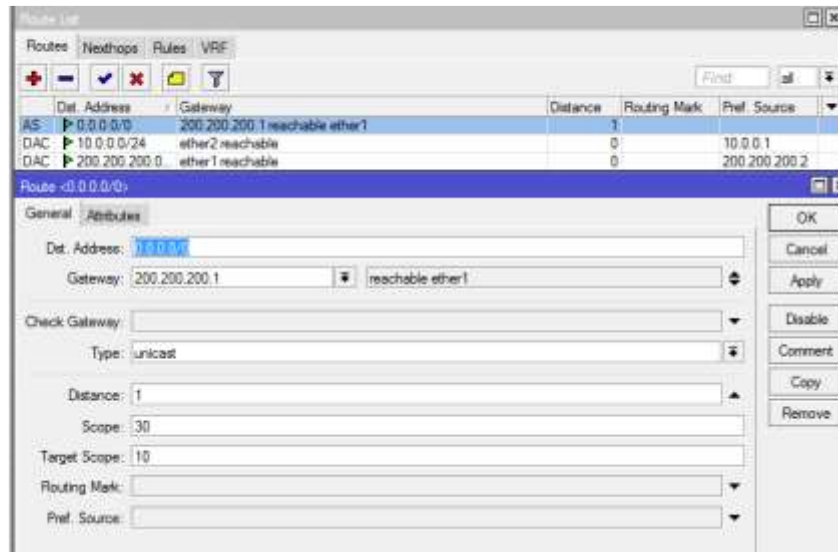
Pada router ini penulis menggunakan 2 ether, ether 1 untuk IP Public dan ether 2 untuk IP Local. Langkah memberikan IP Address pada masing - masing interface dengan klik Menu| IP | Address | pada tampilan Address List klik tombol + warna merah.



Gambar 4. 9 Pengaturan IP Address

9. Pengaturan Route Table

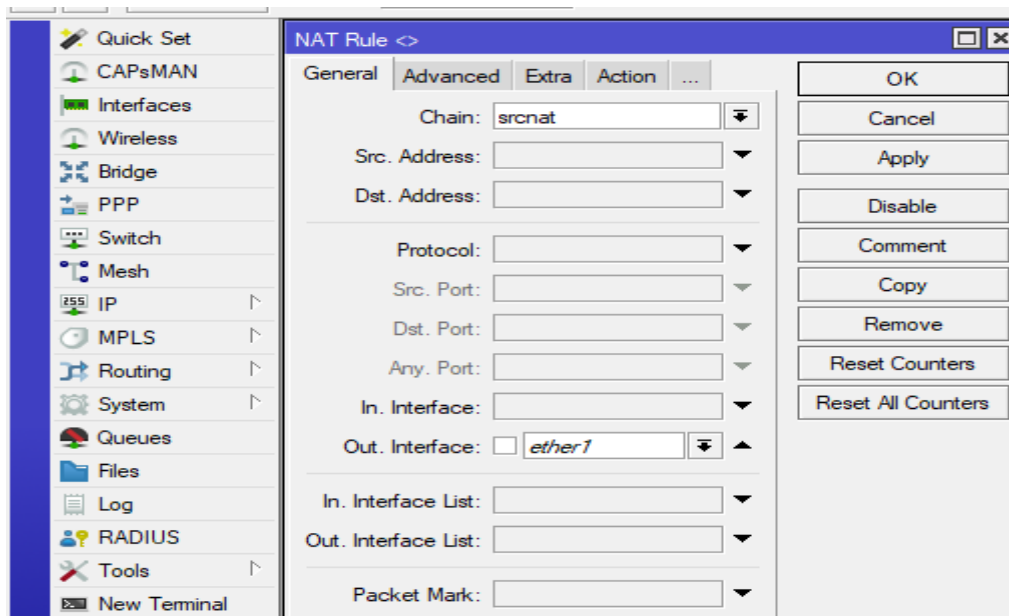
Set Route pada Mikrotik Router bertujuan untuk menentukan jalur gateway dari jaringan lokal ke jaringan yang terkoneksi internet. Dengan cara klik Menu IP| Routes| pada tampilan Route List klik tombol + warna merah untuk menambahkan gateway seperti gambar:

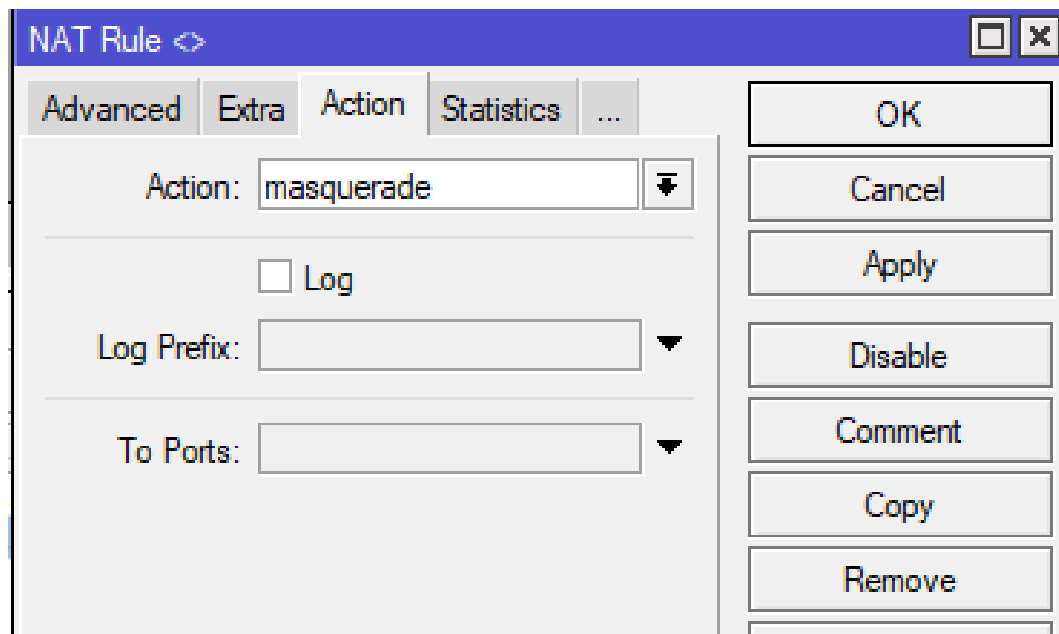


Gambar 4. 10 Pengaturan Route Table

10. Pengaturan Firewall NAT

Network Address Translation (NAT) adalah suatu metode menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP. Klik Menu IP | Firewall | NAT. Setting seperti gambar:

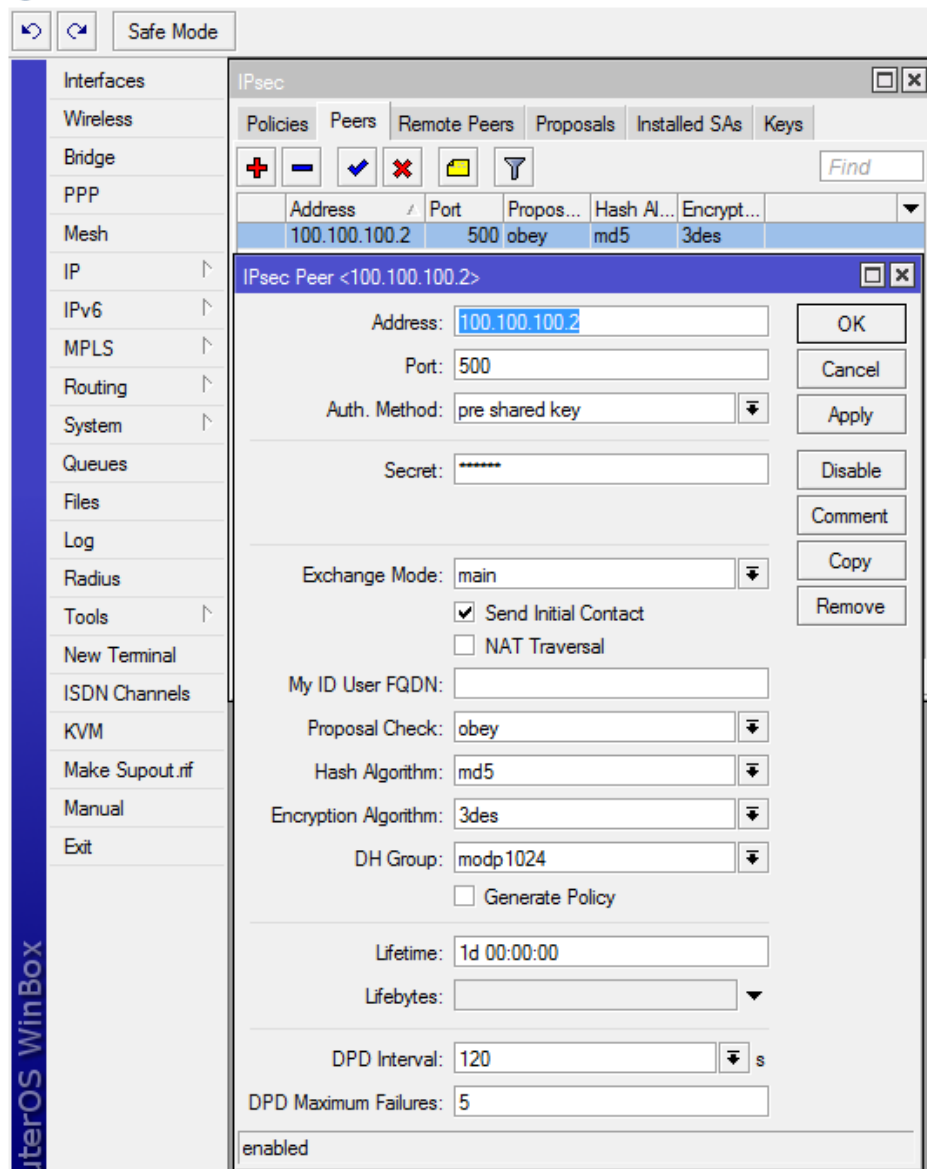




Gambar 4. 11 Pengaturan Nat

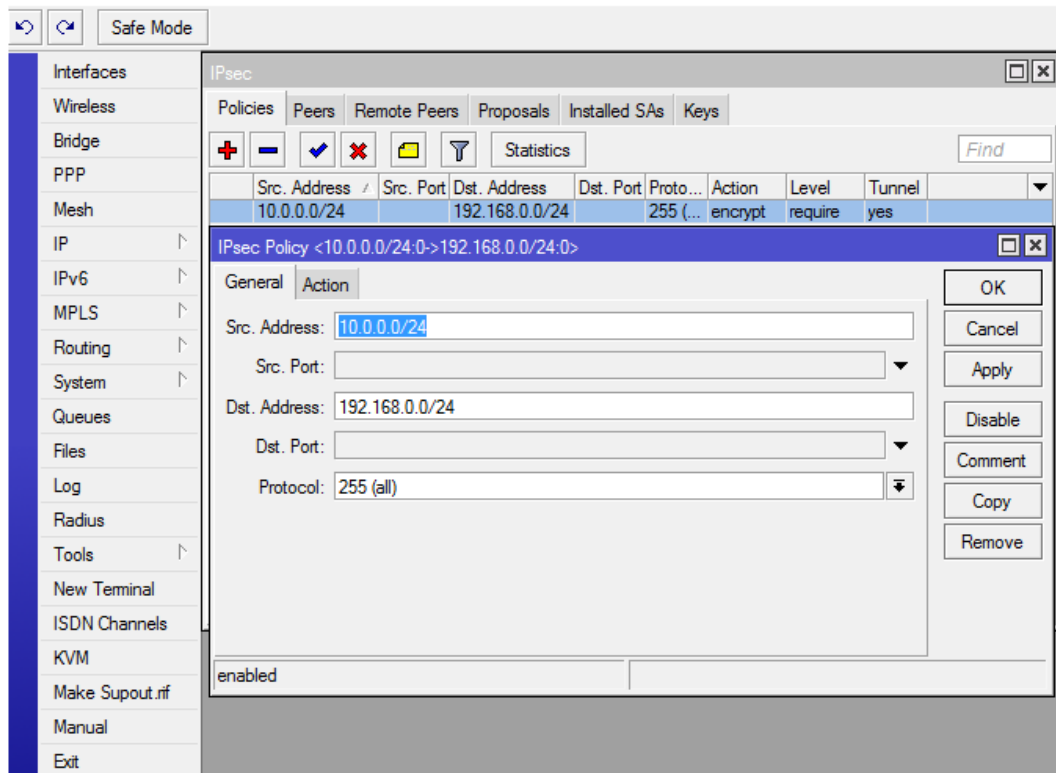
11. Pengaturan IPSec Peer

IPSec adalah sebuah protokol yang digunakan untuk mengamankan transmisi datagram dalam sebuah internetwork berbasis TCP/IP. Klik Menu IP|IPSec|Peers. Setting seperti gambar :



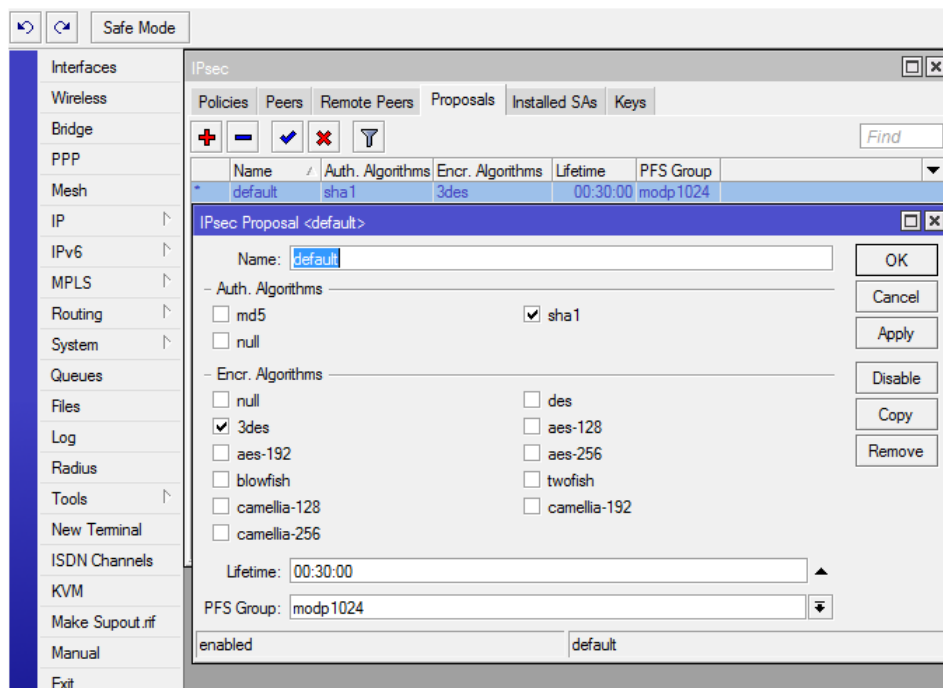
Gambar 4. 12 Pengaturan IPsec Peer

Selanjutnya setting pada Tab IPsec Policy, tambahkan juga parameter pada tampilan berikut :



Gambar 4. 13 Pengaturan IPsec Policy

Selanjutnya setting pada Tab IPsec | Proposal |, tambahkan juga parameter pada tampilan berikut :



Gambar 4. 14 Pengaturan IPsec Proposal

4.3 Konfigurasi VPN PPTP

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. Fitur ini sudah termasuk dalam *package* PPP sehingga 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 bisa menggunakan Laptop/PC sebagai PPTP Client.

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

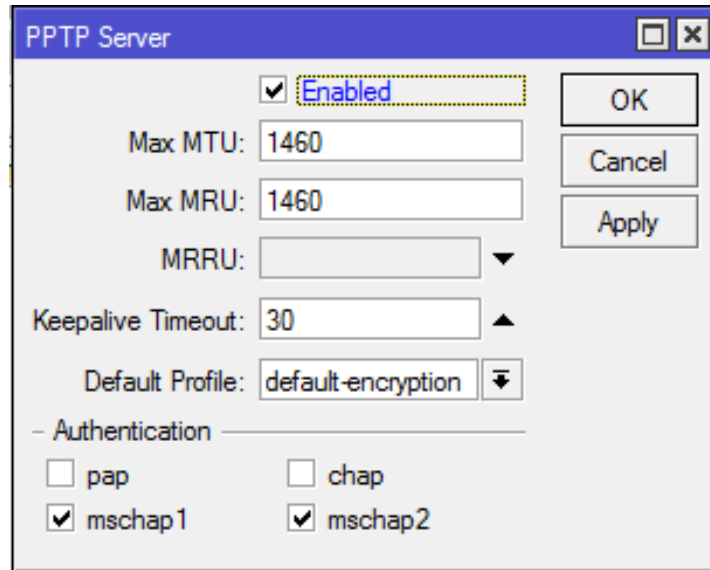
Router SMK dan Router Rumah terhubung ke internet via *ether 1* dan PC pada masing-masing jaringan lokal terhubung ke *Ether 2*. Remote client juga sudah terhubung ke internet. Konfigurasi agar Router SMK dan jaringan LAN A bisa diakses dari Router Rumah dan jaringan LAN B serta Remote Client. Langkah-langkah setting PPTP dengan Winbox sebagai berikut:

a. Konfigurasi PPTP Server

Berdasarkan topologi yang telah dijabarkan, yang menjadi pusat dari link PPTP (konsentrator) adalah Router SMK , maka harus melakukan setting PPTP Server pada router tersebut.

Enable PPTP Server

Langkah pertama yang harus dilakukan adalah mengaktifkan PPTP server. Masuk pada menu **PPP->Interface->PPTP Server** . Gunakan profile "*Default-encryption*" agar jalur VPN terenkripsi.



Gambar 4. 15 Enable PPTP Server

b. Secret

Pada tahap ini, kita bisa menentukan **username** dan **password** untuk proses autentikasi Client yang akan terkoneksi ke PPTP server. Penggunaan huruf besar dan kecil akan berpengaruh.

-**Local Address** adalah alamat IP yang akan terpasang pada router itu sendiri (Router SMK / PPTP Server) setelah link PPTP terbentuk

-**Remote Address** adalah alamat IP yang akan diberikan ke Client setelah link PPTP terbentuk.

Contoh konfigurasi sebagai berikut. Arahkan agar menggunakan profile "*Default-Encryption*"

PPP Secret <pptpsmk>

Name: pptpsmk

Password: 123

Service: pptp

Caller ID:

Profile: default-encryption

Local Address: 10.0.0.1

Remote Address: 10.0.0.2

Routes:

Limit Bytes In:

Limit Bytes Out:

Last Logged Out: Sep/13/2021 16:18:31

Last Caller ID: 100.100.100.254

Last Disconnect Reason: hung up

enabled

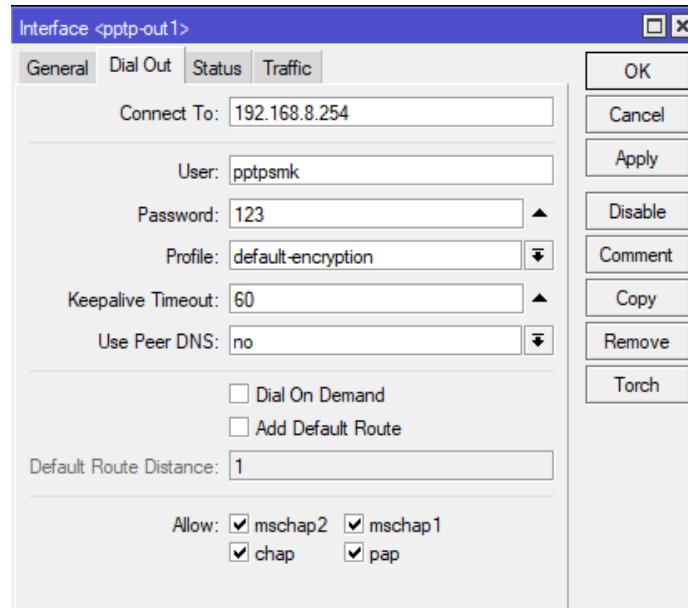
Gambar 4. 16 New PPP Secret Server

Sampai disini, konfigurasi Router SMK (*PPTP Server*) sudah selesai, lakukan konfigurasi di sisi client.

Client Router Rumah

Langkah-langkah untuk melakukan konfigurasi Client PPTP pada Router Mikrotik adalah sebagai berikut :

Tambahkan interface baru PPTP Client, lakukan dial ke IP Public Router SMK (*PPTP server*) dan masukkan username dan password sesuai pengaturan secret PPTP Server.



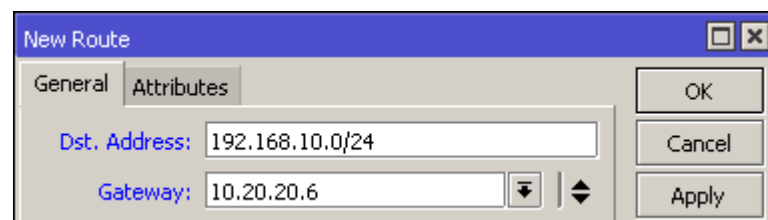
Gambar 4. 17 Dial Out PPTP

Setelah koneksi PPTP terbentuk, akan muncul IP Address baru di kedua Router yang menempel di interface pptp sesuai dengan pengaturan Secret pada PPTP server

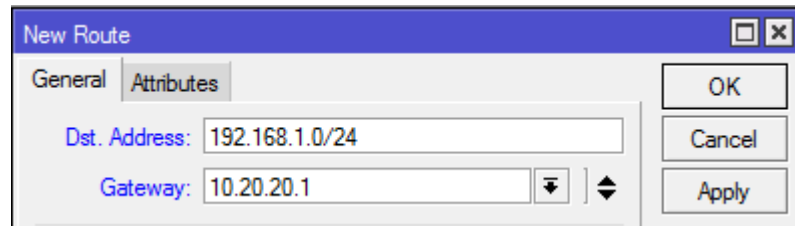
c. Static Route

koneksi VPN antar router sudah terbentuk, akan tetapi antar jaringan lokal belum bisa saling berkomunikasi. Agar antar jaringan lokal bisa saling berkomunikasi, perlu menambahkan routing static dengan konfigurasi

- **dst-address** : jaringan local Router lawan
- **gateway** : IP PPTP Tunnel pada kedua router.



Gambar 4. 18 Penambahan static route di Router SMK



Gambar 4. 19 Penambahan static route di Router Rumah

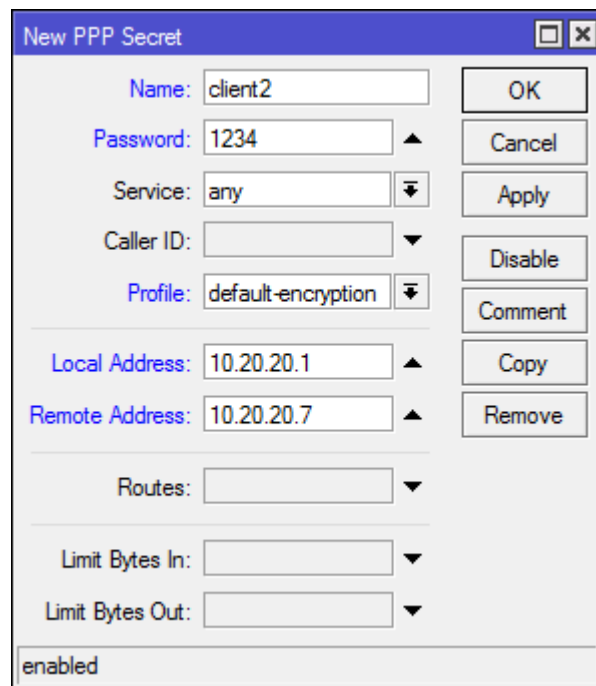
d. Mobile Client

Client PPTP tidak harus menggunakan Router. Seperti pada topologi jaringan di atas, ada sebuah Remote Client (Laptop) yang akan melakukan koneksi VPN ke Router SMK.

Maka perlu membuat Secret baru pada PPTP server untuk autentikasi remote client tersebut.

e. Secret

username = **client2** ; password = **1234** ; Local Address = **10.20.20.1** ; Remote Address = **10.20.20.7**



Gambar 4. 20 PPP Secret Client

Kemudian melakukan konfigurasi PPTP Client pada Laptop. Langkah-

langkahnya berbeda pada tiap OS. Berikut konfigurasi PPTP Client untuk OS Windows 7.

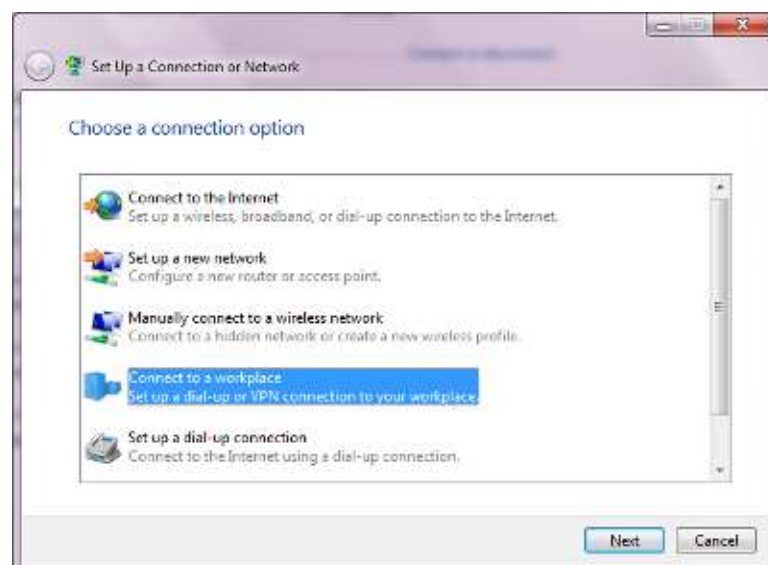
f. Konfigurasi PPTP Client Windows 7

Pastikan Laptop sudah bisa akses internet. Masuk pada menu Network and Sharing Center, kemudian create koneksi baru dengan memilih **Set up new connection or network**.



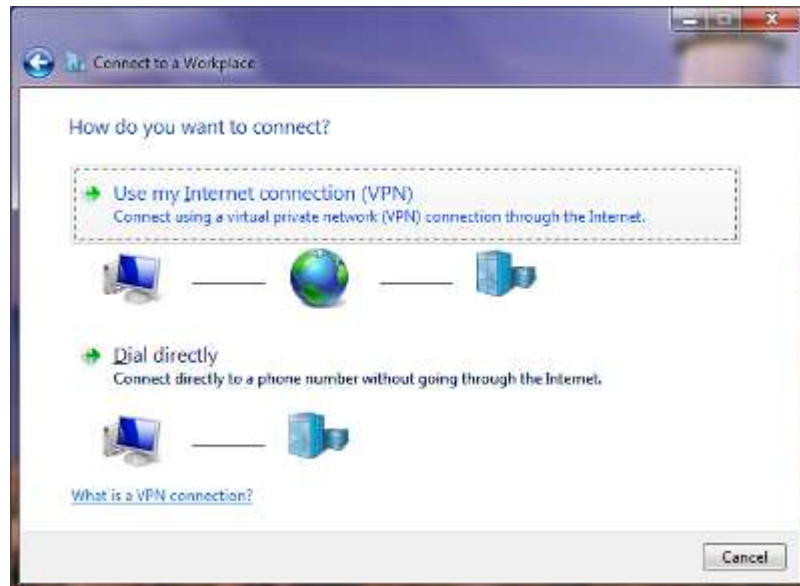
Gambar 4. 21 Set up new connection or network.

Pada tampilan window selanjutnya, pilih **Connect to a workplace** , lalu klik next.



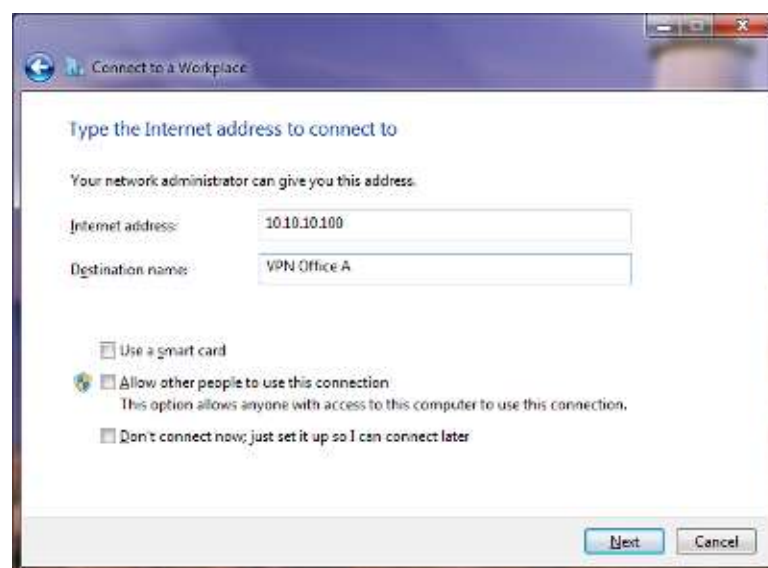
Gambar 4. 22 Connect to a workplace

Kemudian, pilih **Use My Internet Connection (VPN)**



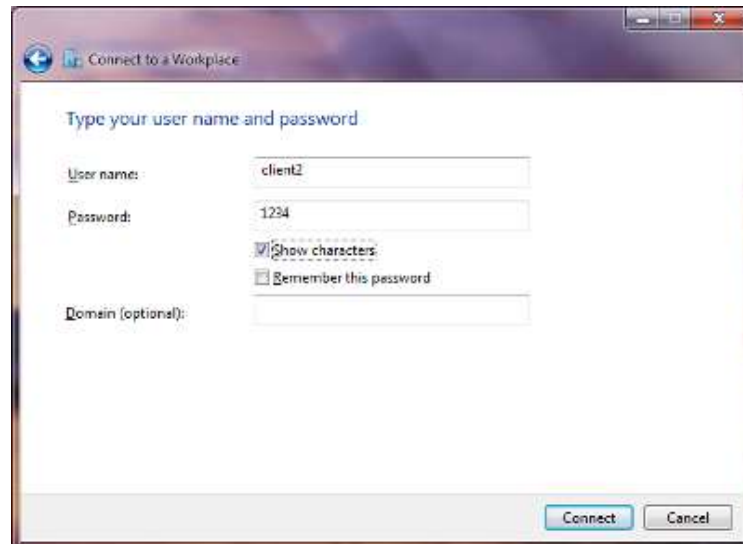
Gambar 4. 23 Use My Internet Connection (VPN)

Pada langkah berikutnya memasukkan ke IP Address untuk melakukan koneksi. Sesuai topologi , maka masukkan IP address public Router SMK. Destination name adalah parameter untuk memberikan nama pada interface VPN yang sedang dibuat.



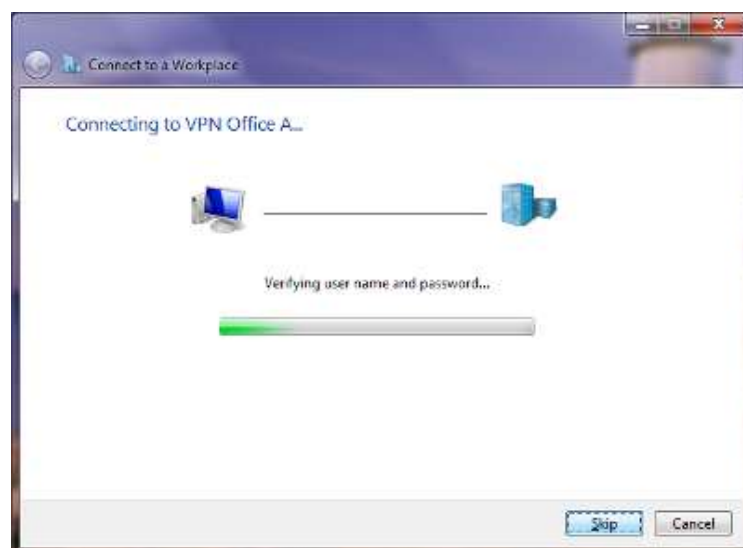
Gambar 4. 24 Connect Interface VPN

Selanjutnya masukkan username dan password sesuai pengaturan Secret yang ada di PPTP server. Lalu klik Connect.



Gambar 4. 25 Connect Workspace Client

Akan ada proses autentikasi, tunggu sampai selesai.



Gambar 4. 26 Autentikasi VPN

Jika sudah selesai, di laptop muncul interface baru dengan nama VPN SMK dan terpasang IP address yang mengambil dari ip-pool Remote Address sesuai dengan pengaturan profile dan Secret pada PPTP Server.

Sampai disini koneksi VPN dari Laptop ke Router SMK sudah terbentuk. Laptop sudah bisa akses ke Router SMK dan Jaringan LAN A.

Untuk melakukan remote ke Router SMK tinggal memasukkan IP address Router yang terpasang setelah link VPN terbentuk, yaitu IP address 10.20.20.1

4.4 Pengujian Jaringan

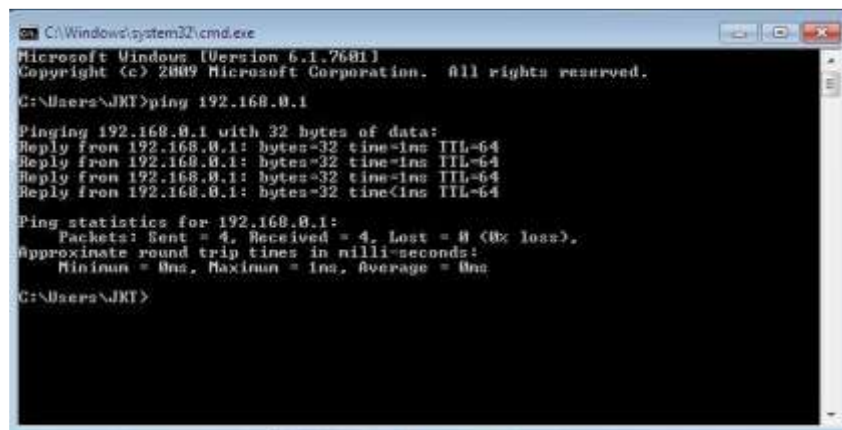
Dalam hal membangun jaringan komputer perlu dilakukan sebuah pengujian terhadap jaringan yang telah dibangun sebelumnya, hal ini berguna untuk memastikan bahwa semua sistem yang telah dibuat berjalan dengan baik dan sesuai dengan yang direncanakan.

4.3.1. Pengujian Jaringan Awal

Pada sub bab ini akan dilakukan beberapa pengujian awal diantaranya tes koneksi dari client ke *gateway*, dari client ke router dengan cara ping.

1. Ping dari client ke gateway pada kantor SMK.

Pada pengujian ini penulis mencoba melakukan tes koneksi dari salah satu client ke *gateway* dengan cara ping pada SMK.



```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\JKI>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\JKI>
  
```

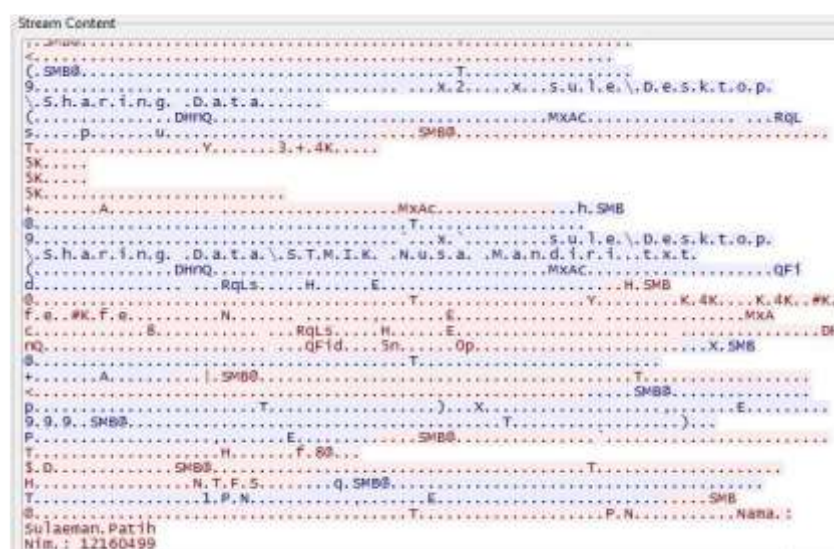
Gambar 4. 27 Ping dari Client ke Gateway pada Kantor SMK

2. Ping dari client ke router pada SMK

Pada percobaan kali ini penulis akan mencoba menghubungkan atau melakukan tes koneksi antara client dengan router yang berada pada jaringan lokal.

Dari hasil pengujian diatas terlihat bahwa hasil tes koneksi dapat terhubung dengan baik dan tidak ada data yang lost.

Pada pengujian ini penulis mencoba melakukan pengiriman data dalam jaringan lokal, kemudian dilakukan analisa paket data jaringan menggunakan *wireshark*. Hasil dari paket data sebelum menggunakan VPN dengan aplikasi *wireshark* yaitu terlihat bahwa data yang dikirim bisa terbaca, seperti gambar dibawah ini :

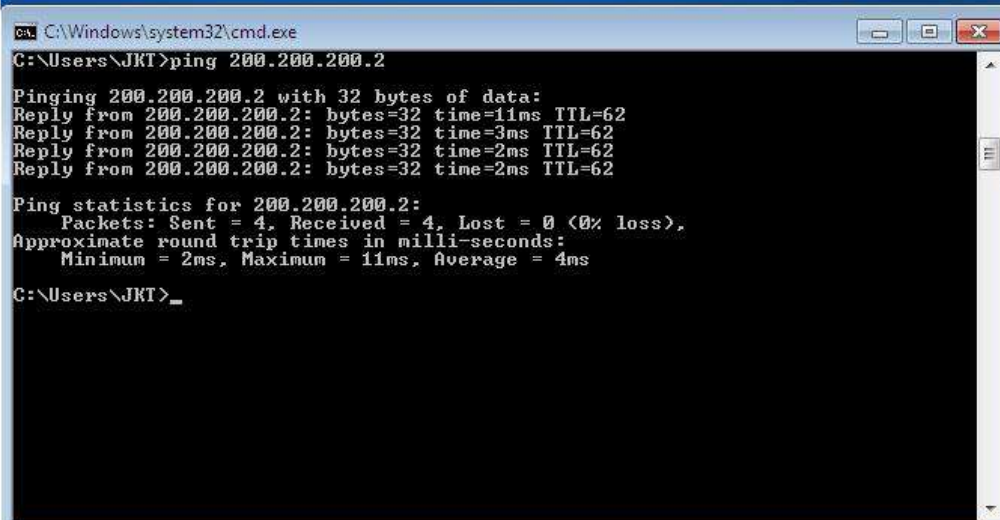


Gambar 4. 29 Analisa sebelum menggunakan VPN

4.5 Pengujian Jaringan Akhir

Pada pengujian jaringan akhir penulis akan mencoba melakukan tes koneksi dengan melakukan ping dari client yang berada di kantor SMK ke client Rumah, dari client kantor SMK ke router Rumah begitu juga sebaliknya, dan melakukan *tracert* dari SMK ke Rumah.

1. Ping dari client SMK ke router Rumah



```
C:\Windows\system32\cmd.exe
C:\Users\JKT>ping 200.200.200.2

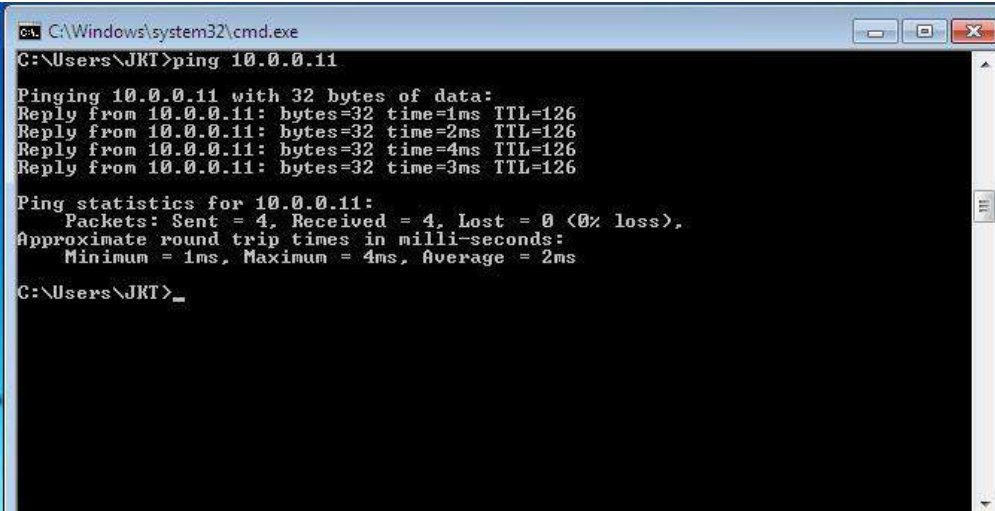
Pinging 200.200.200.2 with 32 bytes of data:
Reply from 200.200.200.2: bytes=32 time=11ms TTL=62
Reply from 200.200.200.2: bytes=32 time=3ms TTL=62
Reply from 200.200.200.2: bytes=32 time=2ms TTL=62
Reply from 200.200.200.2: bytes=32 time=2ms TTL=62

Ping statistics for 200.200.200.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 11ms, Average = 4ms

C:\Users\JKT>_
```

Gambar 4. 30 Ping dari client kantor SMK ke router Rumah

2. Ping dari client SMK ke client rumah



```
C:\Windows\system32\cmd.exe
C:\Users\JKT>ping 10.0.0.11

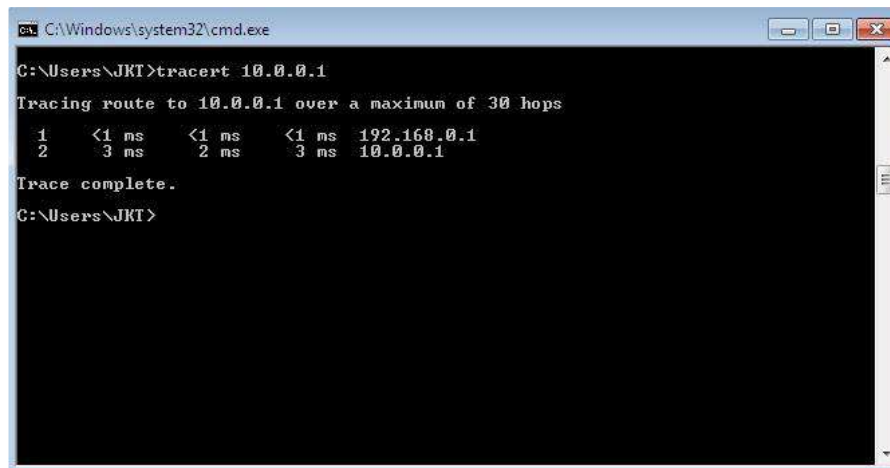
Pinging 10.0.0.11 with 32 bytes of data:
Reply from 10.0.0.11: bytes=32 time=1ms TTL=126
Reply from 10.0.0.11: bytes=32 time=2ms TTL=126
Reply from 10.0.0.11: bytes=32 time=4ms TTL=126
Reply from 10.0.0.11: bytes=32 time=3ms TTL=126

Ping statistics for 10.0.0.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms

C:\Users\JKT>_
```

Gambar 4. 31 Ping dari client SMK ke client rumah

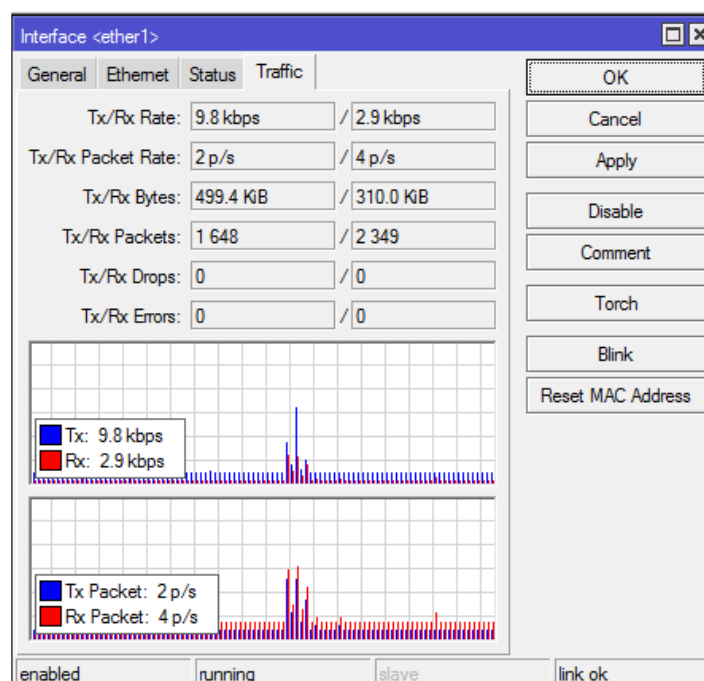
3. Tes koneksi dengan tracert dari SMK ke rumah



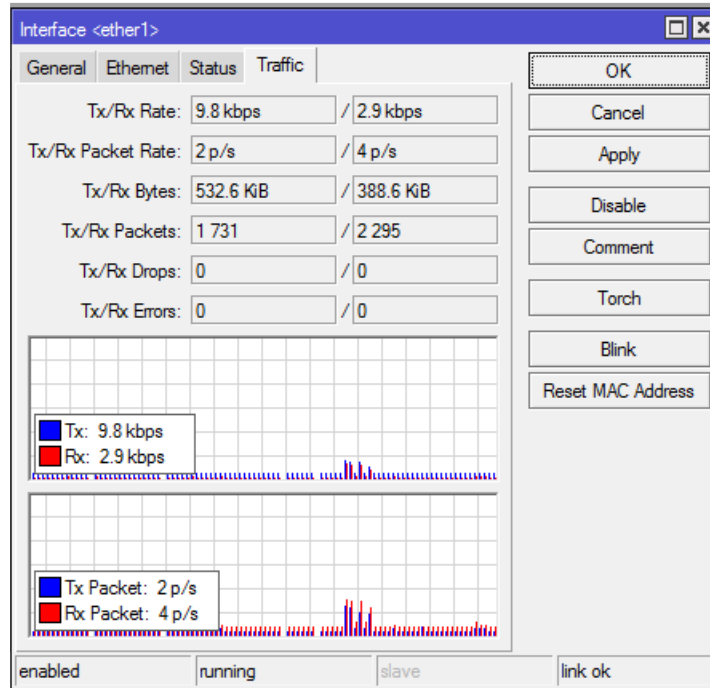
Gambar 4. 32 Tes Tracert dari SMK ke rumah

Pada pengujian diatas terlihat bahwa koneksi berjalan dengan baik, dari client SMK bisa terhubung langsung ke rumah, hal ini bisa saling melakukan tukar menukar data. Pengujian dengan traceroute untuk melihat rute yang dilewati sebuah data ke tempat tujuan dan ini terlihat bahwa rute melewati tunnel yang telah dibuat dengan VPN.

4. Grafik Transfer Data



Gambar 4. 33 Grafik Transfer Data pada Router SMK

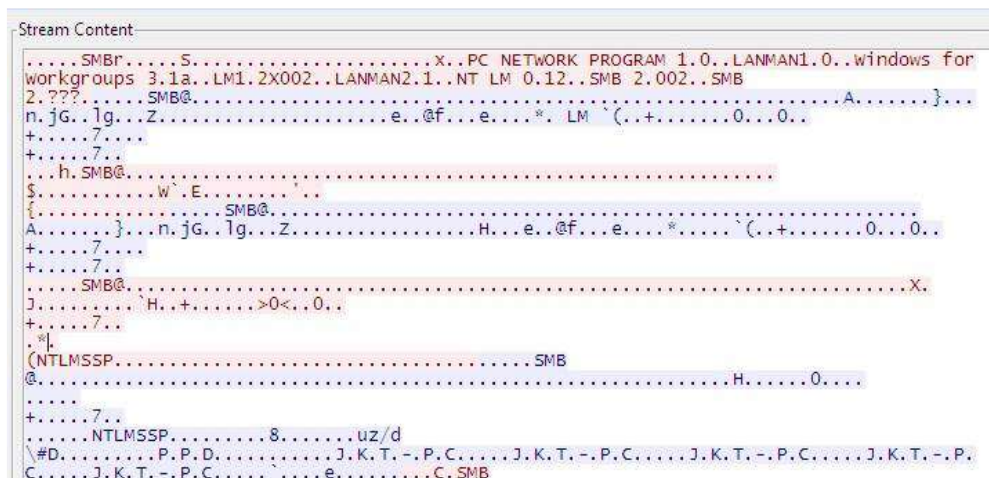


Gambar 4. 34 Grafik Transfer Data pada Router Rumah

5. Tes Pengiriman Data

Dalam pengujian ini penulis mencoba melakukan pengiriman data dari PC rumah ke PC SMK dengan koneksi VPN. Dan setelah dilakukan konfigurasi dengan akhirnya pengiriman berhasil.

Dibawah ini merupakan gambar dari analisa yang melewati jaringan SMK menggunakan wireshark. Dari hasil analisa ini bahwa data yang dikirim telah terenkripsi.



Gambar 4. 35 Analisa Paket Data

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Beberapa kesimpulan dari hasil yang didapat selama penulis melakukan analisa dan implementasi jaringan di SMK Islam Manbaul Hikmah Luwunragi adalah sebagai berikut :

1. Untuk mengatasi masalah pertukaran data yang penting dengan ukuran besar dapat diterapkan sistem jaringan VPN metode PPTP pada jaringan komputer. Dengan diterapkannya jaringan VPN, maka antara SMK dan rumah akan saling terhubung, sehingga memberikan akses data yang baik, cepat dan aman.
2. Untuk mengelola suatu jaringan yang kompleks dengan biaya yang relatif murah kita dapat memanfaatkan sarana sekolah tanpa harus merubah topologi jaringan yang sudah ada.
3. Penulis mengetahui tentang pemanfaatan mikrotik routerOS yang bisa digunakan untuk membuat jaringan virtual private network (VPN).
4. Jaringan Virtual Private Network (VPN) memberikan kemudahan bagi pegawai yang memiliki hak akses untuk mengakses jaringan lokal sekolah dari mana saja, karena VPN terhubung ke internet.
5. Rancangan jaringan VPN menggunakan Mikrotik sebagai sarana pengaksesan file serta kontrol jaringan jarak jauh untuk SMK Islam Manbaul Hikmah Luwunragi yang aman dapat diimplementasikan dengan baik.

5.2 Saran

Dari perancangan dan implementasi jaringan VPN yang telah dilakukan, maka penulis ingin memberikan saran-saran terhadap implementasi tersebut. Sebagai alternatif pemikiran yang dapat dijadikan masukan yang nantinya akan sangat berguna, dengan harapan agar dapat meningkatkan kinerja secara optimal dalam hal sistem jaringan komputer.

Saran-saran yang diberikan penulis sebagai berikut:

1. Perlu dilakukannya analisa dan pengecekan terus menerus terhadap jaringan virtual private network (VPN) yang telah dirancang agar komunikasi data dapat terhubung dengan baik dan aman.
2. Perlu dilakukan analisis terus menerus terhadap pengujian keamanan jaringan, karena semakin berkembangnya teknologi semakin tinggi pula tingkat ancaman keamanan terlebih dari serangan para peretas.

DAFTAR PUSTAKA

- [1] H. Yuliandoko, Jaringan Komputer Wire dan Wireless Beserta Penerapannya, Yogyakarta: CV BUDI UTAMA, 2018.
- [2] Siyamta, Administrasi Server Jaringan, Jakarta: Kemdikbud, 2020.
- [3] E. Mufida, D. Irawan dan G. Chrisnawati, "Remote Site Mikrotik VPN Dengan Point To Point Tunelling Protocol (PPTP) Studi Kasus Pada Yayasan Teratai Global Jakarta," *Jurnal Matrik*, vol. 16, pp. 9-19, 2017.
- [4] H. Supendar, "Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik," *BINA INSANI ICT JOURNAL*, vol. 3, no. 1, pp. 85-98, 2016.
- [5] Athaillah, Panduan Singkat Menguasai Mikrotik untuk pemula, Jakarta: Media Kita, 2013.
- [6] D. Setiawan, Sistem Keamanan Komputer, Jakarta: PT Elex Media Komputindo, 2017.
- [7] P. S. Utomo, "Analisis kinerja VPN Berbasis Mikrotik Pada Proses Kompresi-Dekompresi Dan Enkripsi-Dekripsi di Bandingkan VPN Berbasis Open Source," *Jurnal Teknik Informatika*, pp. 10-16, 2020.
- [8] F. Sjafrina, P. D. Arnesia dan A. Aqim, "Rancang Bangun Jaringan VPN Berbasis IPSEC Menggunakan Mikrotik Routerboard Pada PT. Zahir Internasional," dalam *Seminar Nasional Teknologi Informasi dan Komunikasi STI&K (SeNTIK)*, Jakarta, 2019.
- [9] Sutarti dan A. Alfiyansyah, "Analisis dan Implementasi Sistem Monitoring Koneksi Internet Menggunakan The Dude Di STIKOM Al Khairiyah," *Jurnal Sistem Informasi*, vol. 4, no. 6, pp. 39-45, 2017.
- [10] Kustanto dan T. D. Saputro, Belajar Jaringan Komputer berbasis Mikrotik OS, Yogyakarta: Gava Media, 2015.
- [11] A. Ramadhan, Recipe Kitchen Mikrotik, Jakarta: ID-Networkers, 2018.

- [12] Supono, "MTCNA for Training," ID-Networkers, Jakarta, 2017.
- [13] A. Novianto, Administrasi Sistem Jaringan, Jakarta: Penerbit Erlangga, 2018.



YAYASAN MANBAUL HIKMAH LUWUNGRAGI
SMK ISLAM MANBAUL HIKMAH LUWUNGRAGI

Jl. Raya Luwungragi No.35 RT 04/07 Kec. Bulakamba Kab. Brebes
E-mail : smkislammanbaulhikmah@yahoo.co.id Telp. 0857 1066 6685

SURAT KETERANGAN

No. 743/422/2021

Yang bertanda tangan di bawah ini Kepala SMK Islam Manbaul Hikmah Luwungragi menerangkan bahwa :

Nama : Ari Irkham Fauzi
NIM : 55201190031
Fakultas : Teknik
Program Studi : Teknik Informatika
Judul Skripsi : Implementasi Virtual Private Network (VPN) Server Menggunakan Mikrotik Untuk Remote Access Di SMK Islam Manbaul Hikmah Luwungragi

Yang bersangkutan telah melakukan penelitian di SMK Islam Manbaul Hikmah Luwungragi pada tanggal 18 Maret s.d. 18 April 2021.

Surat Keterangan ini diberikan agar dipergunakan sebagaimana semestinya.

Luwungragi, 22 April 2021

Kepala Sekolah,

Dewi Kentera Ati, S.Pd

LEMBAR WAWANCARA
SMK ISLAM MANBAUL HIKMAH LUWUNGRAGI

Judul Penelitian : Implementasi Virtual Private Network (VPN) Server Menggunakan Mikrotik Untuk Remote Access Di Smk Islam Manbaul Hikmah Luwungragi

Tempat Penelitian : Laboratorium SMK Islam Manbaul Hikmah Luwungragi

Nama Mahasiswa : Ari Irkham Fauzi

NIM : 55201190031

Program Studi : Teknik Informatika

Petunjuk : Berikan tanda centang (✓) pada kolom isian "Ya" atau "Tidak" sesuai dengan jawaban atas pertanyaan yang diajukan pada kolom pertanyaan !

Tabel Instrumen Observasi

No	Aspek Pengamatan	Jawaban Anda		Keterangan
		Ya	Tidak	
1	Apakah SMK Islam Manbaul Hikmah Luwungragi Membutuhkan Pengamanan Jaringan?	✓		Sangat membutuhkan
2	Jaringan wifi memiliki keamanan yang baik?		✓	Belum ada keamanan jaringan yang baik
3	Terdapat Pembagian Jaringan di Laboratorium SMK Islam Manbaul Hikmah Luwungragi?	✓		Ada Pembagian Jaringan
4	Kecepatan internet yang kurang baik di SMK Islam Manbaul Hikmah Luwungragi?		✓	Kadang mengalami kesulitan saat mengakses jaringan
5	Terdapat internet di SMK Islam Manbaul Hikmah Luwungragi?	✓		Ya ada internet

Tabel Instrumen Wawancara

No	Pertanyaan	Hasil Wawancara
	Salam Pembuka	
1	Jaringan apa yang digunakan pada SMK Islam Manbaul Hikmah Luwunragi?	Jaringan LAN dan Wireless
2	Berapa kecepatan akses jaringan yang digunakan pada SMK Islam Manbaul Hikmah Luwunragi?	20 Mbps
3	Masalah apa yang terjadi pada jaringan wireless pada SMK Islam Manbaul Hikmah Luwunragi?	Terjadinya konektifitas lambat loading
4	Apakah pada SMK Islam Manbaul Hikmah Luwunragi sudah menggunakan VPN untuk mengamankan jaringan wireless?	Belum
5	Berapa unit pc yang digunakan pada SMK Islam Manbaul Hikmah Luwunragi	25 PC
6	Perangkat-perangkat jaringan apa saja yang digunakan pada SMK Islam Manbaul Hikmah Luwunragi?	Switch, Router Mikrotik, Access Point
7	Selama ini pernahkah menemukan solusi agar akses jaringannya menjadi lancar ketika tidak di sekolah?	Belum Pernah
8	Jika hadir sebuah pengembangan jaringan untuk keamanan dan akses dari mana saja, untuk siapakah sasaran objek pemakai yang tepat?	Untuk Karyawan dan Staff yang memerlukan akses dari mana saja, terutama tim IT
	Salam Penutup	

DOKUMENTASI PENELITIAN



Wawancara dengan teknisi IT SMK Islam Manbaul Hikmah Luwungragi



Observasi dan wawancara karyawan dan guru



Analisis Data dan Perancangan Jaringan



Proses Instalasi Jaringan Mikrotik



Perancangan Jaringan menggunakan Aplikasi



Foto Bersama Tim IT