BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi dibidang sistem informasi semakin berkembang pesat. Hal ini dibuktikan dengan semakin banyaknya penemuan-penemuan yang merubah cara penyampaian dalam menyampaikan suatu informasi. Sementara itu dengan berkembangnya teknologi semakin banyak pula konsumsi listrik yang digunakan. Dalam melakukan efisiensi sumber daya listrik dapat dimulai dari kebutuhan rumah tangga masing-masing, kebutuhan sumber daya listrik di kantor ataupun kebutuhan sumber daya listrik disekitar. Namun, kegiatan *monitoring* dan perhitungan sumber daya listrik sekarang masih dilakukan manual jadi alangkah lebih baik bila cara *Monitoring* dan perhitungan sumber daya listrik dilakukan secara otomatis oleh suatu sistem karena kemungkinan dengan adanya sistem *monitoring* energi listrik akan mendorong agar lebih hemat menggunakan energi listrik. Sehingga dirasa perlu untuk mengembangkan sistem o*n-grid*. Sistem *on-grid* merupakan sebuah sistem yang menghubungkan antara listrik yang dihasilkan oleh sebuah pembangkit yang menghasilkan energi terbaharui dengan energi listrik yang tidak dapat diperbaharui.

Didalam pengerjaan sistem *on-grid* maka sangat dibutuhkan sistem jaringan yang dapat mengakomodir sistem secara keseluruhan agar dapat bekerja dengan baik. Sistem jaringan yang digunakan adalah metode *Virtual Private Network* (VPN) sebagai media penghubung dari perangkat *monitoring* menuju server yang sudah ada.

1.2 Rumusan Masalah

Adapun terdapat beberapa rumusan masalah pada Proyek akhir ini :

1.Bagaimana cara kerja topologi sistem jaringan yang dibentuk?

2. Apa saja yang digunakan untuk mengimplementasikan jaringan?

2.Bagaimana hasil pengujian QOS?

1.3 Manfaat

Adapun beberapa manfaat dari proyek akhir ini, yaitu :

1.Mempermudah pemonitoran arus listrik;

2.Mengetahui hasil pengujian QOS yang sesuai dengan standar ITU-T G.114;

1.3 Tujuan

Adapun beberapa tujuan dalam pembuatan jaringan sistem on-grid, yaitu :

1.Membuat jaringan untuk melancarkan proses pemonitoran daya listrik;

2. Dapat mengetahui hasil QOS pada *tunnel* pada jaringan yang dibuat sesuai standar ITU-T G.114

3.Dapat mengetahui hasil QOS jaringan VPN secara keseluruhan sesuai dengan standar ITU-T G.114;

1.4 Batasan Masalah

1.Sistem ini menggunakan mikrotik dan akses point;

2.Sistem ini menggunakan metode tunneling L2TP;

3.Sistem ini menggunakan i*psec* sebagai protocol pengamanannya;

1.5 Metode Penyelesaian Masalah

Langkah-langkah yang akan ditempuh dalam menyelesaikan Proyek Akhir ini adalah:

1.Studi Literatur

a. Pencarian dan pengkajian teori mengenai pembuatan jaringan beserta cara kerjanya dari berbagai literatur serta sumber yang bermacam-macam seperti buku, internet, jurnal dan wawancara langsung.

b. Pengumpulan data-data dan spesifikasi sistem yang dipakai untuk pembuatan sistem jaringan.

2. Analisis Masalah

Melakukan analisa dari teori yang telah didapat dengan bermacam-macam sumber sehingga mendapatkan hasil yang semaksimal mungkin.

3. Perancangan dan realisasi

Membuat jaringan berdasarkan parameter-parameter yang diinginkan.

4. Simulasi Sistem

Berdasarkan standar yang ada, tahap selanjutnya adalah melakukan simulasi sistem untuk melihat kinerja sistem tersebut.

5. Pengujian dan Perbaikan Sistem

Jika sistem telah berjalan, maka akan didapat keberhasilan maupun ketidakberhasilan dari simulasi sistem tersebut, sehingga dilakukan perbaikan sistem jika didapati sistem tersebut belum berjalan secara maksimal.

1.6 Sistematika Penulisan

Adapun sistematika penulisan Proyek Akhir ini dibagi menjadi beberapa bab, yaitu:

BAB I PENDAHULUAN

Berisi latar belakang permasalahan, tujuan, perumusan masalah, pembatasan masalah dan asumsi yang digunakan, serta metode penelitian yang dilakukan.

BAB II DASAR TEORI

Berisi konsep dasar mengenai jaringan yang digunakan dalam pendukung pembuatan perancangan dan implementasi jaringan pada sistem on-grid beserta cara kerjanya.

BAB III PERANCANGAN DAN REALISASI SISTEM

Berisi tentang perancangan dan jaringan pada sistem on-grid.

BAB IV PENGUJIAN DAN ANALISIS

Bab ini membahas mengenai perancangan dan implementasi jaringan yang telah diimplementasikan. Pengujian dan analisis akan mengacu pada terkirim atau tidak hasil data dari perangkat monitoring menuju server.

BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan atas hasil kerja yang telah dilakukan serta saran-saran.

BAB II

DASAR TEORI

2.1 Sistem *On-grid*[1]

Sistem *On-grid* adalah suatu konsep yang dibangun untuk memenuhi kebutuhan energi listrik yang di masa sekarang dan masa mendatang sudah menjadi kebutuhan primer. Dimana komunikasi terjadi dua arah antara produsen listrik serta konsumennya telah diimplementasikan menggunakan teknologi analog bertahun-tahun lamanya dan merupakan teknologi yang menggabungkan bidang informasi, komunikasi dan tenaga listrik yang bertujuan untuk menghemat atau efisiensi penggunaan tenaga listrik.

Sistem On-grid berpotensi menjadi revolusi dalam penghematan energi. Contohnya, dengan teknologi ini, pengguna rumahan tidak hanya bertindak sebagai konsumen, tetapi juga bisa sebagai produsen. Teknologi ini masih butuh banyak pengembangan di sisi bidang informasi, komunikasi serta tenaga listriknya, belum lagi dari sisi bisnis dan kebijakan pemerintah.

Sistem On-grid juga memiliki pusat penyimpanan energi yang berfungsi mengantisipasi perubahan beban secara mendadak ataupun fluktuasi pada pembangkit. Dalam pengaplikasiannya Sistem *On-grid* membutuhkan jaringan komputer dan komunikasi data memainkan peranan penting dalam sistem. sistem komunikasi yang digunakan harus mempunyai kecepatan memadai, memiliki dua arah komunikasi, dan terintegrasi secara penuh. Salah satu keunggulan konsumen yang terhubung dengan Sistem *On-grid* dapat memilih kapan menggunakan sumber listrik yang PLN atau sumber listrik terbaharui, karena saat harga sumber listrik dari PLN diperhitungkan lebih mahal dari pada sumber listrik terbaharui maka secara otomatis akan mengambil sumber listrik dari energi terbaharui begitu juga bila energi terbaharui dirasa kurang cukup memenuhi kebutuhan maka akan memakai sumber listrik PLN.

2.2 Router Mikrotik RB 750[2]

RB750 adalah produk *routerboard* yang sangat praktis dan serbaguna dikarenakan memiliki ukuran yang kecil namun memiliki kemampuan yang sudah cukup memenuhi

persyaratan untuk membangun suatu jaringan dalam kapasitas kecil seperti kantor atau rumahan.

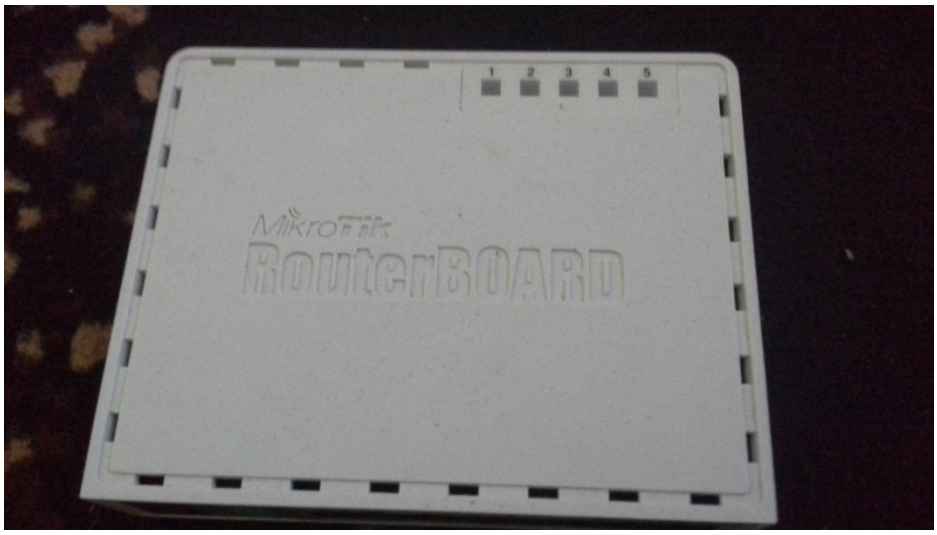
Gambar 2.1 Mikrotik Router RB 750

Tabel 2.1 Spesifikasi lengkap routerboard 750

Spesifikasi RB 750	
Product Code	RB750
CPU	AR7241 400MHz
Main Storage/NAND	64MB
RAM	32MB
Lan Ports	5
Switch Chip	1
Integrated Wireless	No
Power Jack	10-28V
POE Input	10-28V
Dimentions	113x89x28mm
Operating System	Router OS
Temperature Range	-40..+55C
Router OS License	Level 4

2.3 Router Mikrotik Rb 951-2n[8]

RB951-2n adalah produk routerboard yang sangat praktis dan serbaguna sama seperti RB 750 routerboard ini memiliki ukuran yang kecil namun memiliki kemampuan yang sudah cukup memenuhi persyaratan untuk membangun suatu jaringan dalam kapasitas kecil seperti kantor atau rumahan dan juga routerboard ini sudah dilengkapi oleh Wifi card sehingga didalam mengkonfigurasinya sudah dapat melalui via nirkabel.



Gambar 2.2 Router Mikrotik RB 951 2n

Tabel 2.2 Spesifikasi Rb 951-2N

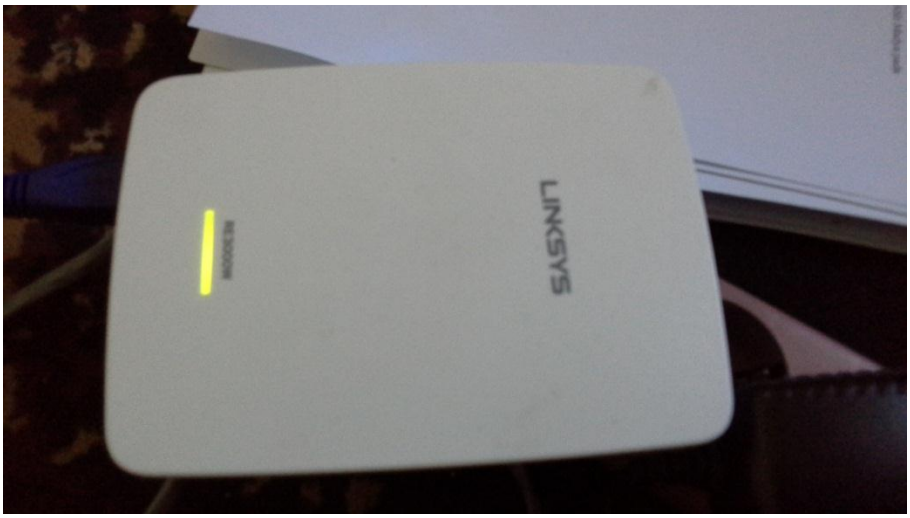
Spesifikasi RB 951-2N	
Product Code	RB951-2N
CPU speed	300MHz
RAM	32MB
LAN ports	5
Integrated Wireless	Yes
Wireless standards	802.11b/g/n
PoE	8-28V DC on Ether1
Temperature range	-20C .. +50C
RouterOS License	Level4
Antenna gain	1.5dBi
TX power	17dBm

2.4 Linksys RE 3000W

Linksys RE 3000W adalah sejenis *wireless extender* dimana fungsi dari alat ini adalah menangkap dan meneruskan sinyal *wifi* agar lebih besar daerah jangkauannya. Spesifikasinya sebagai berikut :

Tabel 2.3 Spesifikasi Linksys RE 3000W

Spesifikasi Linksys RE 3000W	
Konektivitas	2.4GHz
Fast Ethernet	(10/100) Bridge
Input	USB
Ukuran (L x W x H cm)	1x1x25



Gambar 2.3 Linksys RE 3000W

2.5 *Virtual Private Network*[6]

Virtual Private Network atau biasa dikenal dengan VPN adalah sebuah koneksi *private* melalui jaringan publik atau internet, dari kosa katanya dapat dijabarkan sebagai berikut : virtual network berarti jaringan yang terjadi hanya bersifat *virtual*. *Private* yaitu jaringan yang terbentuk bersifat *private* dimana tidak semua orang bisa mengaksesnya. Data yang dikirimkan terenkripsi sehingga tetap rahasia meskipun melalui jaringan publik. Jika menggunakan VPN seolah-olah membuat jaringan didalam jaringan atau biasa disebut *tunnel*. VPN merupakan perpaduan antara teknologi *tunneling* dan enkripsi. Teknologi

VPN menyediakan tiga fungsi utama untuk penggunanya. Fungsi utama tersebut adalah sebagai berikut:

1.*Confidentiality* (Kerahasiaan) Teknologi VPN memiliki sistem kerja mengenkripsi semua data yang lewat melaluinya. Dengan adanya teknologi enkripsi ini, maka kerahasiaan Anda menjadi lebih terjaga. Biarpun ada pihak yang dapat menyadap data Anda yang lalu-lalang, namun belum tentu mereka bisa membacanya dengan mudah karena memang sudah diacak. Dengan menerapkan sistem enkripsi ini, tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data Anda dengan mudah.

2.*Data Integrity* (Keutuhan Data) Ketika melewati jaringan Internet, sebenarnya sudah berjalan sangat jauh melintasi berbagai negara. Di tengah perjalanannya, apapun bisa terjadi terhadap isinya. Baik itu hilang, rusak, bahkan dimanipulasi isinya oleh orang-orang iseng. VPN memiliki teknologi yang dapat menjaga keutuhan data yang Anda kirim agar sampai ke tujuannya tanpa cacat, hilang, rusak, ataupun dimanipulasi oleh orang lain.

3.*Origin Authentication* (Autentikasi Sumber) Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi *source* datanya. Kemudian alamat source data ini akan disetujui jika proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang semestinya. Tidak ada data yang dipalsukan atau dikirimkan oleh pihak-pihak lain.

2.6 *Layer Two Protocol* (L2TP)[5]

L2TP adalah salah satu protokol *tunneling* yang memadukan dua buah protokol tunneling, yaitu L2F (*Layer 2 Forwarding*) milik Cisco dan PPTP milik Microsoft (Gupta, 2003). L2TP memungkinkan penggunanya untuk tetap dapat terkoneksi dengan jaringan lokal milik mereka dengan *policy* keamanan yang sama dan dari manapun mereka berada, melalui koneksi VPN atau VPDN. Koneksi ini sering kali dianggap sebagai sarana memperpanjang jaringan lokal milik penggunanya, namun melalui media publik.

Namun, teknologi tunneling ini tidak memiliki mekanisme untuk menyediakan fasilitas enkripsi karena memang benar-benar murni hanya membentuk jaringan tunnel. Fasilitas

enkripsi disediakan oleh protokol enkripsi yang lewat di dalam tunnel. Selain itu, apa yang lalu-lalang di dalam tunnel ini dapat ditangkap dan dimonitor dengan menggunakan *protocol analizer*.

2.7 Winbox[6]

Winbox adalah sebuah *utility* yang digunakan untuk melakukan *remote* ke server mikrotik kita dalam mode GUI. Jika untuk mengkonfigurasi mikrotik dalam text mode melalui PC itu sendiri, maka untuk mode GUI yang menggunakan winbox ini kita mengkonfigurasi mikrotik melalui komputer client.

Mengkonfigurasi mikrotik melaui winbox ini lebih banyak digunakan karena selain penggunaannya yang mudah juga tidak harus menghapal perintah-perintah console. fungsi winbox yang lain adalah sebagai berikut:

1. mengkonfigurasi mikrotik
2. untuk mengkonfigurasi *bandwidth* jaringan internet
3. untuk memblokir sebuah situs

2.8 *Internet Protocol Security* (IPsec)[7]

Internet Protocol Security (IPsec) adalah protokol untuk mengamankan Internet Protocol (IP) komunikasi dengan otentikasi dan enkripsi setiap paket IP dari sebuah sesi komunikasi. IPsec juga mencakup protokol untuk mendirikan otentikasi bersama antara agen pada awal sesi dan negosiasi kunci kriptografi yang akan digunakan selama sesi.

IPsec merupakan *end-to-end security* skema yang beroperasi di layer internet dari *Internet Protocol Suite* . Hal ini dapat digunakan dalam melindungi aliran data antara sepasang *host* (*host-to-host*), antara sepasang *gateway* keamanan (jaringan-jaringan), atau antara gateway keamanan dan *host* (jaringan-*to-host*) .

IPsec adalah penerus dari standar ISO *Layer Security* Jaringan Protokol (NLSP). NLSP didasarkan pada protokol SP3 yang diterbitkan oleh NIST , tetapi dirancang oleh proyek Sistem Jaringan Data Aman dari *National Security Agency* (NSA). IPsec secara resmi ditetapkan oleh *Internet Engineering Task Force* (IETF) dalam serangkaian Request for

Comment dokumen menangani berbagai komponen dan ekstensi. Ini menentukan ejaan dari nama protokol IPsec.

2.9 Standarisasi ITU-T[4]

ITU-T (ITU *Telecommunication Standardization Sector*) merupakan badan khusus PBB di bidang telekomunikasi. ITU-T bertanggung jawab untuk mempelajari teknis, operasi dan penerbitan *Recommendation* dengan maksud untuk standarisasi telekomunikasi di seluruh dunia. Dalam proyek akhir ini yang digunakan adalah standar ITU-T G.114 dimana G *series* merupakan standar untuk menentukan sistem transmisi dan media, sistem *digital* serta jaringan. Berikut akan ditampilkan rumus yang digunakan dan standarisasi dari setiap parameter yang digunakan :

1. **Throughput**

   Berikut rumusan untuk mendapatkan nilai dari parameter *Throughput* :

$$\text{Throughput} = \frac{\text{Pr}}{\text{1detik}} \quad \text{Pkt/det}\ldots..0 \leq t \leq T \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2.1)$$

Pr = Paket yang diterima (paket)

T = Waktu simulasi (detik)

t = Waktu pengambilan sampel (detik)

2. ***Delay***

   Berikut rumusan untuk mendapatkan nilai dari parameter *Delay* :

$$\text{Delay} = \left(\frac{\text{Tr-Ts}}{\text{Pr}}\right) \text{ detik}\ldots\ 0 \leq t \leq T \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2.2)$$

Tabel 4.2 Standar Kualitas ITU-T G.114 untuk *Delay*

Nilai *Delay*	Kualitas
0-150ms	Baik
150-400ms	Cukup,Masih dapat diterima
>400ms	Buruk,tidak dapat diterima

1. *Packet Loss*

Berikut rumusan untuk mendapatkan nilai dari parameter *packet loss* :

$$\text{Packet Loss} = \left(\frac{Pd}{Ps}\right) \quad X\ 100\%... \ 0 \leq t \leq T$$

……(2.2)

Pd = Paket yang mengalami *drop* (paket)

Ps = Paket yang dikirim (paket)

T = Waktu simulasi (detik)

t = Waktu pengambilan sampel (detik)

Terdapat juga standar kualitas dari *packet loss* yang dapat dikategorikan dalam beberapa kategori berdasarkan ITU-T G.114 yaitu sebagai berikut :

Tabel 4.3 Standar Kualitas ITU-T G.114 untuk *Packet Loss*

Nilai *Delay*	Kualitas
0-0.5%	Sangat Baik
0.5-1.5%	Baik
>1.5%	Buruk

Tr = Waktu penerimaan paket (detik)

Ts = Waktu pengiriman paket (detik)

Pr = Paket yang diterima (paket)

T = Waktu simulasi (detik)

t = Waktu pengambilan sampel (detik)

2.10 Wireshark

WireShark adalah sebuah *software* gratis yang digunakan untuk analisis jaringan yang biasa digunakan oleh *network administrator* untuk menganalisa kinerja jaringan termasuk protocol di dalamnya. Tujuan dari monitoring dengan wireshrak adalah sebagai berikut :

1. Memecahkan masalah jaringan
2. Memerikasa Keamanan Jaringan
3. Men-*debug* implementasi protokol
4. Mempelajari protokol jaringan internal

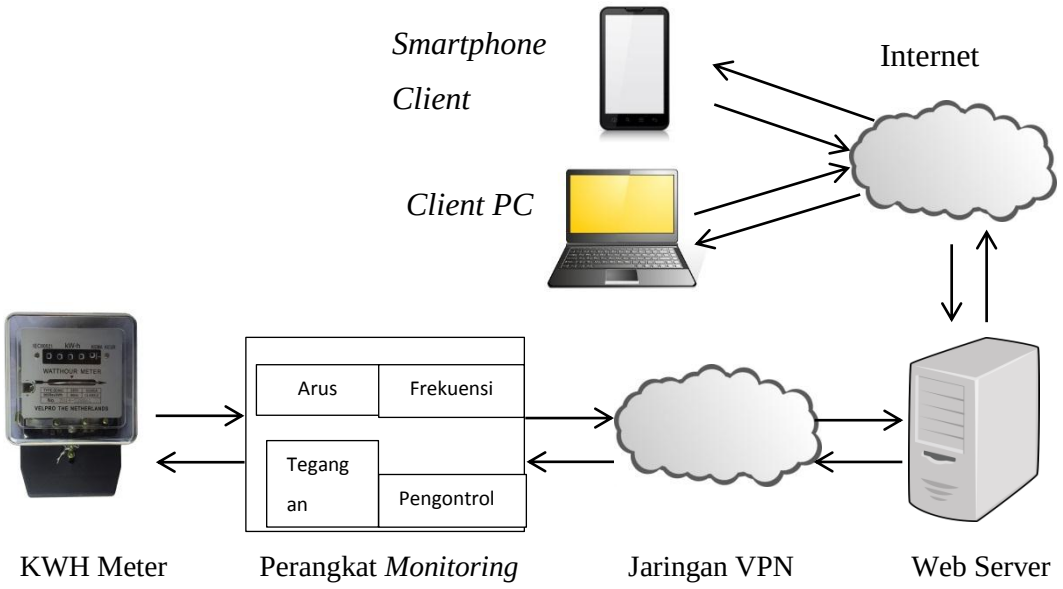
Wireshark memiliki beberapa keuntungan, diantaranya dapat memantau paket paket data yang diterima dari internet. Wireshark bekerja pada layer Aplikasi. Yaitu layer terakhir dari OSI Layer. Dengan menggunakan protocol protocol di layer application HTTP, FTP, TELNET, SMTP, DNS kita dengan mudah memonitoring jaringan yang ada.

BAB III

PERANCANGAN DAN REALISASI SISTEM

3.1 Cara Kerja Sistem On-Grid Secara Umum

Didalam rancangan secara umum, sistem On-grid yang dibuat terdiri dari 4 bagian yaitu perangkat monitoring yang berfungsi sebagai pengukur arus,tegangan dan juga frekuensi yang dicatat oleh KWH meter. Bagian yang kedua adalah sistem jaringan untuk memfasilitasi proses pengiriman data dari perangkat monitoring dan kontrol menuju ke web server. Bagian yang ketiga adalah sistem web server dimana didalam web server terjadi pengolahan data dari perangkat monitoring dan kontrol agar data-data yang tadinya tidak beraturan menjadi lebih rapi untuk dilihat oleh *client*. Bagian yang terakhir adalah aplikasi pengontrolan yang terdapat didalam aplikasi *smartphone* dimana,dengan aplikasi tersebut *user* dapat mengontrol penggunaan energi listrik yang ada di rumah atau kantor tempat dimana alat perangkat monitoring dan pengontrol terpasang. Salah satu contoh yang dibuat adalah mengatur energi listrik pada lampu. Untuk lebih jelasnya dapat dilihat di gambar dibawah.



Gambar 3.1 Cara kerja sistem *on-grid* secara umum

Dari gambar 3.1 sudah digambarkan cara kerja sistem *on-grid* secara umum, dan sekarang akan dijelaskan bagaimana proses sistem *on-grid* yang telah dibangun. Berikut ini adalah proses sistem *on-grid* yang telah dibangun :

1. Perangkat *monitoring* dan pengontrol mencatat arus, frekuensi dan tegangan dari KWH Meter
2. Data-data yang dicatat dikirimkan melalui jaringan VPN yang sudah dibuat menuju server
3. Didalam *website*, *user* dapat melihat penggunaan arus, frekuensi dan tegangan
4. Didalam aplikasi android yang sudah dibuat, *user* dapat melihat penggunaan arus, frekuensi dan tegangan pada smartphone dan juga user dapat mengontrol penggunaan energi listrik yang dicontohkan dengan penggunaan lampu.

Dalam pengerjaan proyek akhir ini dilakukan dengan berkelompok. Sehingga setiap orang mendapatkan satu bidang, Jadi didalam buku ini akan lebih banyak mengulas tentang sistem jaringan yang digunakan.

3.2 Spesifikasi Awal

Sistem on-grid adalah sistem yang sedang berkembang, sehingga bukan tidak mungkin sistem ini akan banyak digunakan. Oleh sebab itu diperlukan suatu sistem jaringan yang cukup baik agar sistem on-grid secara keseluruhan dapat bekerja secara maksimal, terutama didalam proses pengiriman data dari perangkat *monitoring* menuju *web server*. Karena jika ditahap ini data tidak sampai ke *web server*, maka sistem on-grid tidak akan berjalan.

Dibutuhkan jaringan yang baik dalam hal kualitas juga dalam hal *maintenance* jaringan untuk memudahkan bila terjadi kesalahan pada jaringan. Dibutuhkan jaringan yang fleksibel agar mudah untuk menambah atau mengurangi perangkat. Juga dibutuhkan alokasi ip yang memiliki kapasitas besar untuk menampung banyak alat monitoring. Contoh kasus sebagai berikut apabila didalam satu komplek terdiri dari 50 rumah, 40 rumah sudah memakai sistem *on-grid*. Dua bulan kemudian 3 rumah ingin menggunakan sistem on-grid juga, sehingga diperlukan instalasi perangkat dan jaringan. Jika jaringan tidak fleksibel atau jika alokasi ip yang disediakan sedikit maka instalasi jaringan akan menyulitkan.

Untuk memenuhi kebutuhan tersebut maka digunakanlah jaringan *Virtual Private Network* (VPN) dengan metode *tunneling,* dan juga topologi yang digunakan adalah star, untuk alasan menggunakan sistem tersebut adalah sebagai berikut :

3.2.1 *Virtual Private Network*

Dalam proses pengiriman data, salah satu yang paling penting adalah keamanan data. Sehingga dalam proyek akhir ini digunakan VPN sebagai metode pengiriman data. Dengan teknologi VPN hanya *user* yang memiliki hak akses yang dapat masuk kedalam jaringan, keuntungan yang kedua dengan penggunaan vpn adalah jangkaun jaringan lokal yang dimiliki pihak pengelola *on-grid* akan semakin luas. Sehingga semakin banyak daerah yang dapat menggunakan sistem *on-grid*. Sedangkan bila menggunakan *leased line* akan membutuhkan waktu yang lama untuk membangun jalur koneksi khusus dari perangkat *monitoring* dengan *web server*. Ketiga, penggunaaan VPN dapat mereduksi biaya operasional bila dibandingkan dengan penggunaan *leased line* sebagai cara tradisional untuk mengimplementasikan WAN. 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. VPN menggunakan internet sebagai media komunikasinya. Pihak pengelola hanya membutuhkan kabel dalam jumlah yang relatif kecil untuk menghubungkan perusahaan tersebut dengan pihak ISP (internet service provider) terdekat.

3.2.2 Tunneling

Tunneling atau terowongan merupakan kunci utama pada VPN. Koneksi pribadi dalam VPN dapat terjadi dimana saja selama terdapat tunnel yang menghubungkan pengirim dan penerima data. Dengan adanya *tunnel,* maka tidak diperlukan pengaturan-pengaturan lain yang ada di luar tunnel tersebut, asalkan sumber dari tunnel tersebut dapat menjangkau tujuannya.

3.2.3 Topologi *Star*

Didalam penentuan topologi ditentukan penggunaan topologi *star* sudah cukup baik untuk memenuhi persyaratan sistem on-grid. Karakteristik dari topologi star adalah sebagai berikut :

1. Mudah di kembangkan karena setiap *node* hanya memiliki kabel yang langsung terhubung ke *central node*.

2. Setiap *Node* berkomunikasi secara langsung dengan *central node*. *Traffic* data mengalir dari *node* ke *central node* dan kembali lagi.

3.Jika terjadi kerusakan pada salah satu *node* maka hanya pada *node* tersebut yang terganggu tanpa menggangu jaringan lain.

4. Jika salah satu perangkat monitoring mengalami masalah koneksi, maka perangkat monitoring yang lain tidak akan terkena dampaknya.

Beberapa keuntungan bila menggunakan topologi *star* adalah sebagai berikut :

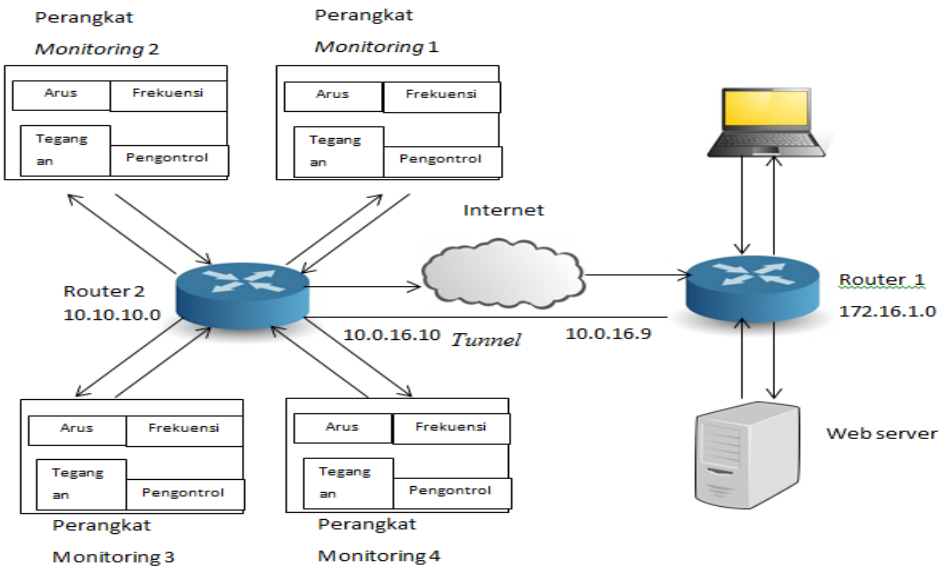
1. Mudah untuk menambah atau mengembangkan koneksi

2. Termasuk mudah dalam melakukan *troubleshooting*

3. Jika terdapat masalah pada salah satu koneksi, maka tidak berdampak pada seluruh jaringan

3.3 Topologi Jaringan VPN

Sesuai dengan spesifikasi awal yang diharapkan maka dibuatlah topologi jaringan seperti gambar dibawah ini yang dapat memenuhi kebutuhan dari sistem *on-grid.*



Gambar 3.2 Topologi Jaringan VPN

Penjelasan topologi diatas adalah sebagai berikut :

1. Server mendapatkan Ip dari router mikrotik 1
2. Didalam mikrotik 1 terjadi konfigurasi *user* dan *password* pembentukan *tunnel*
3. Perangkat *monitoring* 1-4 mendapatkan ip dari router mikrotik 2
4. Didalam mikrotik 2 terjadi konfigurasi *user* dan *password* pembentukan *tunnel*
5. Koneksi *tunneling* berhasil dilakukan

Dalam topologi ini minimal harus memilik 1 ip publik yang permanen. Dalam konfigurasinya dibagi dua konfigurasi yaitu mikrotik di sisi perangkat *monitoring*, dan kedua di sisi server. Pertama untuk konfigurasi mikrotik di sisi server sebagai berikut:

3.3.1 Penghitungan *Subnetmask*

Penghitungan subnetmask pada mikrotik di sisi server sebagai berikut:

Tabel 3.1 Penghitungan Subnetmask disisi Server

Address	172.16.1.0	10101100.00010000.00000001.00000000
Netmask	255.255.255.240	11111111.11111111.11111111.11110000
Network	172.16.1.0/28	10101100.00010000.00000001.00000000 (Class B)
Broadcast	172.16.1.15	10101100.00010000.00000001.00001111
Host Min	172.16.1.1	10101100.00010000.00000001.00000001
Host Max	172.16.1.14	10101100.00010000.00000001.00001110
Hosts/Net	14	

Dari data diatas dapat diambil kesimpulan bahwa IP mikrotik di sisi server dapat menampung *hosts* atau *client* sebanyak 14 alamat dimana alamat IP yang diberikan oleh

mikrotik ke client antara 172.16.1.1 sampai 172.16.1.14 dan alamat IP 172.16.1.0/28 tergabung dalam kelas B. Penghitungan subnetmask pada mikrotik di sisi perangkat *monitoring* sebagai berikut:

Tabel 3.2 Penghitungan Subnetmask disisi perangkat *monitoring*

Address	10.10.10.0	00001010.00001010.00001010 .00000000
Netmask	255.255.255.0	11111111.11111111.11111111 .00000000
Network	10.10.10.0/24	00001010.00001010.00001010 .00000000 (Clas A)
Broadcast	10.10.10.255	00001010.00001010.00001010 .11111111
Host Min	10.10.10.1	00001010.00001010.00001010 .00000001
Host Max	10.10.10.254	00001010.00001010.00001010 .11111110
Hosts/Net	254	

Dari data diatas dapat diambil kesimpulan bahwa IP mikrotik di sisi server dapat menampung hosts atau client sebanyak 254 alamat dimana alamat IP yang diberikan oleh mikrotik ke client antara 10.10.10.1 sampai 10.10.10.254 dan alamat IP 10.10.10.0/24 tergabung dalam kelas B. Penghitungan *subnetmask* pada mikrotik di sisi perangkat *monitoring* sebagai berikut:

3.3.2 Konfigurasi Jaringan

```
/ppp secret disabled=no limit-bytes-in=0 \
limit-bytes-out=0 local-address=10.0.16.9 name=alat1
 password=123456 profile=default \
remote-address=10.0.16.10 routes="" service=l2tp
```

Pada sisi server pertama buat pengguna yang akan terhubung ke server. Sangat diharapkan untuk menggunakan nama dan *password* yang rumit.

```
/interface l2tp-server add disabled=no name=l2tp-in1
user=alat1
```

Lalu buat *server*, namanya bebas namun *user* harus sama dengan nama yang sudah dibuat tadi.

```
/interface l2tp-server server set
authentication=pap,chap,mschap1,mschap2 \
default-profile=default-encryption enabled=yes max-mru=1460 max-
mtu=1460 mrru=disabled
```

Langkah diatas untuk mengaktifkan L2TP Server yang sudah dibuat dilangkah sebelumnya dimana dilangkah ini menentukan autentikasi, menentukan ukuran data terbesar yang dapat diterima dan menentukan ukuran data terbesar yang dapat ditransmisikan.

```
/ip ipsec proposal set default auth-algorithms=sha1
disabled=no enc-algorithms=3des \
lifetime=30m name=default pfs-group=modp1024
```

Langkah ini bertujuan untuk menentukan rancangan-rancangan *ipsec* yang akan dibangun, dalam langkah ini kita dapat menentukan algoritma yang digunakan.

```
/ip ipsec policy add action=encrypt disabled=no dst-
address=10.10.10.0/24 \
ipsec-protocols=esp level=require priority=0
proposal=default protocol=all \
sa-dst-address=10.0.16.10 sa-src-address=10.0.16.9 src-
```

```
address=172.16.1.1/28 tunnel=yes
```

Langkah ini bertujuan untuk menentukan kebijakan apakah pengaturan pengamanan harus diterapkan untuk paket atau tidak. Langkah yang dilakukan dalam langkah ini sebagai berikut: aksi terenkripsi, alamat tujuan adalah 10.0.16.10 dengan IP *prefix* 10.10.10.0/24 , sumber alamat adalah 10.0.16.9, dengan IP *prefix* 172.16.1.0/28, dan yang terakhir adalah mengijinkan penggunaan mode terowongan

```
/ip ipsec peer add address=10.0.16.10/32 auth-method=pre-
shared-key \
dh-group=modp1024 disabled=no dpd-interval=disable-dpd dpd-
maximum-failures=1 \
enc-algorithm=3des exchange-mode=main generate-policy=no
hash-algorithm=sha1 \
lifebytes=0 lifetime=1d my-id-user-fqdn="" nat-traversal=no
proposal-check=obey \
secret=123456 send-initial-contact=yes
```

Didalam tahap *ipsec peer*, terjadi proses pengaturan konfigurasi yang digunakan untuk membangun koneksi antara *Internet Key Exchange*. Koneksi ini kemudian akan digunakan untuk bernegosiasi kunci dan algoritma untuk *Destination Source*.

```
/ip route add disabled=no distance=1 dst-
address=10.10.10.0/28 gateway=10.0.16.10 scope=30 target-scope=10
```

Langkah ditahap ini adalah merouting antara jaringan server menuju tunnel di jaringan milik server. Sementara pengaturan disisi perangkat *monitoring* adalah sebagai berikut :

```
/interface l2tp-hardware add add-default-route=no
allow=pap,chap,mschap1,mschap2 \
connect-to=192.168.43.104 dial-on-demand=no disabled=no max-
mru=1460 \
max-mtu=1460 mrru=disabled name=l2tp-BL password=123456
profile=default-encryption user=alat1
```

Langkah pertama buat akun pengguna yang akan dipakai dalam proses VPN, yang perlu diperhatikan adalah *user* dan *password* harus sesuai dengan apa yang sudah terdaftar didalam mikrotik di sisi server

```
/ip ipsec proposal set default auth-algorithms=sha1
disabled=no enc-algorithms=3des \
lifetime=30m name=default pfs-group=modp1024
```

Langkah ini bertujuan untuk menentukan rancangan-rancangan *ipsec* yang akan dibangun, dalam langkah ini kita dapat menentukan algoritma yang digunakan.

```
/ip ipsec policy add action=encrypt disabled=no dst-
address=172.16.1.0/24 \
ipsec-protocols=esp level=require priority=0
proposal=default protocol=all \
sa-dst-address=10.0.16.9 sa-src-address=10.0.16.10 src-
address=10.10.10.0/28 \
tunnel=yes
```

Langkah ini bertujuan untuk menentukan kebijakan apakah pengaturan pengamanan harus diterapkan untuk paket atau tidak. Langkah yang dilakukan dalam langkah ini sebagai berikut: aksi terenkripsi, alamat tujuan adalah 10.0.16.9 dengan IP *prefix* 172.16.1.0/29, sumber alamat adalah 10.0.16.10, dengan IP *prefix* 10.10.10.0/24, dan yang terakhir adalah mengijinkan penggunaan mode terowongan.

```
/ip ipsec peer add address=10.0.16.9/32 auth-method=pre-
shared-key dh-group=modp1024 \
disabled=no dpd-interval=disable-dpd dpd-maximum-failures=1
enc-algorithm=3des \
exchange-mode=main generate-policy=no hash-algorithm=sha1
lifebytes=0 lifetime=1d \
my-id-user-fqdn="" nat-traversal=no proposal-check=obey
secret=123456 send-initial-contact=yes
```

Didalam tahap *ipsec peer*, terjadi proses pengaturan konfigurasi yang digunakan untuk membangun koneksi antara *Internet Key Exchange*. Koneksi ini kemudian akan digunakan untuk bernegosiasi kunci dan algoritma untuk *Destination Source*.

```
/ip route add disabled=no distance=1 dst-
address=172.16.1.0/24 gateway=10.0.16.9 scope=30 target-
scope=10
```

Langkah ditahap ini adalah mer*outing* antara jaringan perangkat *monitoring* menuju tunnel di jaringan milik perangkat *monitoring.*

3.4 Analisis Kebutuhan Sistem

Kebutuhan untuk implementasi sistem ini dibagi menjadi 2 yaitu kebutuhan perangkat keras (*hardware*) dan perangkat lunak (*software*).

3.4.1 Perangkat lunak (*software*)

1. Winbox

Winbox digunakan sebagai *remote access* untuk mengakses *GUI* router mikrotik

3.4.2 Perangkat keras (*Hardware*)

1. Kabel *Ethernet*

Kabel *Ethernet* digunakan sebagai media penghubung antara mikrotik 1 menuju perangkat *monitoring* dan mikrotik 2 menuju server.

2. Router

Dalam perancangan topologi digunakan router mikrotik RB 750 dan RB 951-2n. Kedua router ini memiliki 5 ports namun RB 951-2n memiliki kelebihan terdapat teknologi *wireless adapter* didalam routernya. Masing-masing Mikrotik digunakan untuk mengkonfigurasi jaringan VPN, *DHCP server* dan juga *tunneling* namun untuk router 1 juga digunakan juga sebagai *gateway* dari *web server* menuju *client*. Kapasitas *client* dari masing-masing router mikrotik tergantung dari seberapa besar data yang dikirim melalui router mikrotik, untuk didalam jaringan *on-grid* yang ukuran datanya tidak terlalu besar maka dari *hardware* dapat menampung setidaknya 200 perangkat monitoring.

3. ***Wireless Extender***

Wireless Extender digunakan untuk menerima sinyal dari *mobile hotspot* yang dipergunakan untuk akses internet dan penghubung ke *tunnel* VPN dikarenakan salah satu mikrotik yang digunakan tidak dapat menerima sinyal dari akses point.

3.5 Sistem Secara Umum

Sementara itu sistem secara umum dari perancangan topologi yang dipakai adalah:

1. *Virtual Private Network* (VPN)

   Dalam penggunaan jaringan, digunakan *virtual private network* karena dalam VPN, proses *routing* data lebih sedikit dari pada membangun jaringan internet biasa. Dengan VPN juga dapat menghemat *bandwidth* yang dipakai. Cukup mudah diterapkan..
2. L2TP/Ipsec

   Didalam penggunaan VPN protokol yang digunakan adalah L2TP/Ipsec karena protocol ini cukup aman, mudah dalam konfigurasi, sudah tersedia pada *platform* perangkat modern.
3. Topologi *star*

   Dalam proyek akhir ini topologi yang digunakan adalah topologi *star* karena topologi ini paling flexibel jadi dalam proses penambahan atau pengurangan alat mengaturnya lebih mudah, topologi ini memiliki kontrol terpusat sehingga mudah dalam mendeteksi kesalahan jaringan.
4. Pemilihan subnet /24 untuk *server* dan /28 untuk perangkat *monitoring*

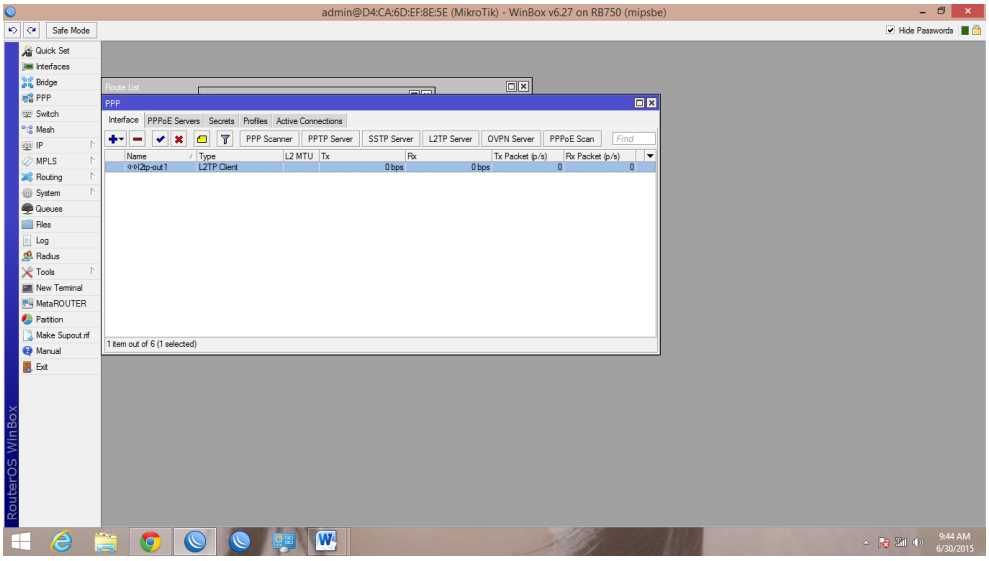
Dalam pemilihan subnet ada 2 subnet yang dipakai dalam proyek akhir ini yaitu /24 yang dipakai untuk server dan juga /28 yang dipakai untuk perangkat monitoring. Alasan memakai /24 untuk server adalah agar server dapat membuat server *monitoring* untuk meringankan beban server, cara kerjanya jika *server* pusat berada di Jakarta,server monitoring berada di Bandung,Bali dan daerah lain untuk meringankan beban server yang diJakarta dan juga agar lebih mudah dalam *troubleshooting* jaringan yang berada di tempat atau kota tersebut. Untuk melihat kapasitas client dari subnet yang dipakai oleh *server* ada di tabel 3.1. Untuk perangkat *monitoring* karena jumlah dari yang diharapkan nanti sangat banyak sehingga diberikan subnet yang dapat menampung hingga 254 buah. Jika kebutuhan ip untuk perangkat monitoring lebih dari

254 buah dapat diatasi dengan radio *access point* yang dipasang di sisa port dari router. Untuk subnet dari tunnel dalam proyek akhir ini menggunakan /32. Hal ini menyebabkan tunnel tidak dapat memiliki *host*.

3.6 Realisasi Sistem

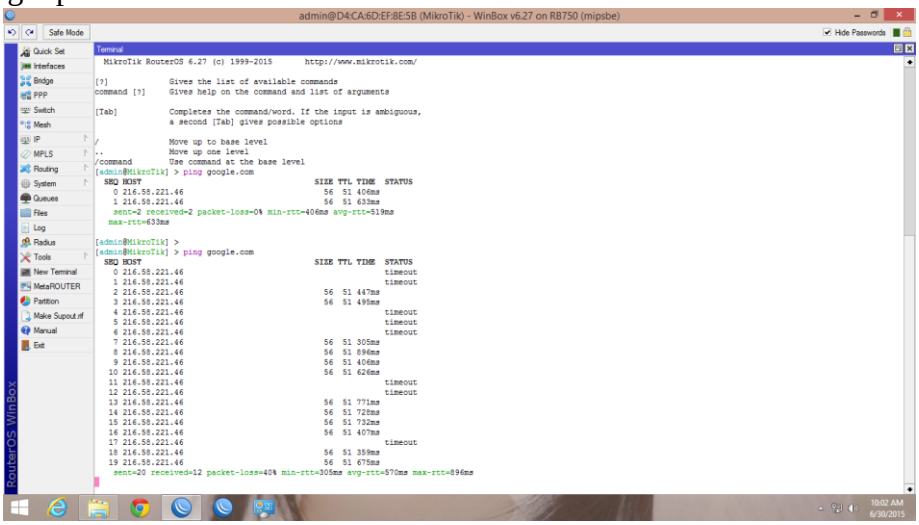
3.6.1 Realisasi Sistem Jaringan

Berikut ini akan dijelaskan realisasi dari sistem jaringan dimulai dari sisi perangkat *monitoring* dan setelah itu dari sisi server.



Gambar 3.4 Tampilan L2TP Client

Gambar 3.4 menjelaskan bahwa L2TP Client sudah terbentuk, dimana fungsi L2TP Client adalah sebagai sisi luar dari jalur VPN yang sudah dirancang. L2TP-out adalah nama yang dipakai untuk L2TP Client.

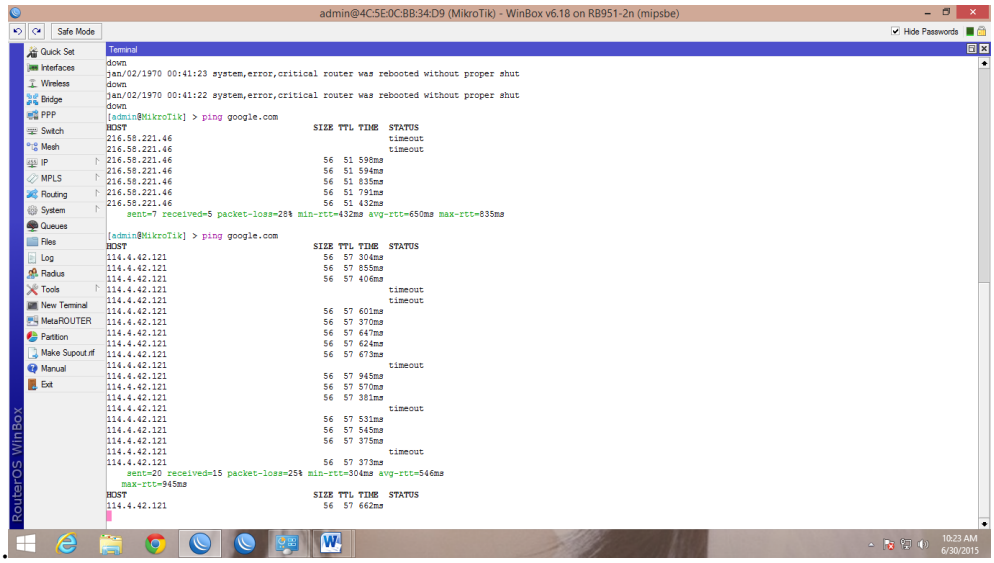


Gambar 3.5 Mikrotik 1

Tampilan diatas menandakan mikrotik dari sisi perangkat *monitoring* dapat terkoneksi keluar hal ini dibuktikan dengan mikrotik dapat melaksanakan perintah ping menuju Ip public luar contohnya google.com dengan hasil dari 20 data yang terkirim yang diterima 12 dan paket yang hilang sebesar 40%

3.6.2 Dari sisi Server

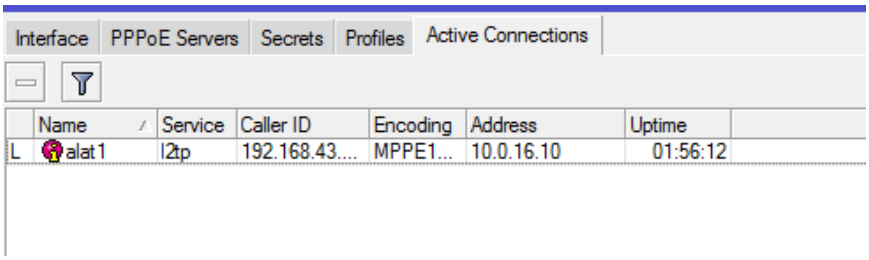
Diatas sudah dijelaskan realisasi jaringan yang dibangun dari sisi perangkat *monitoring*, maka sekarang akan dijelaskan realisasi jaringan yang dibangun dari sisi server.



Gambar 3.6 Mikrotik 2 *connect* internet

Tampilan gambar 3.6 menandakan mikrotik dari sisi perangkat *monitoring* dapat terkoneksi keluar. Hal ini dibuktikan dengan mikrotik dapat melaksanakan perintah ping menuju Ip publik luar contohnya google.com dengan hasil dari 20 data yang terkirim yang diterima 15 dan paket yang hilang sebesar 25%.

Gambar 3.7 adalah tampilan ketika perangkat *monitoring* dapat *login* kedalam jaringan VPN. Dimana alat1 adalah nama dari user perangkat monitoring,caller ID adalah ip public dari perangkat monitoring dan *address* adalah ip yang dipakai dari sisi *tunnel* untuk dapat mengirim data



Gambar 3.7 koneksi aktif di mikrotik server

3.7 Skenario Pengujian

Setelah melakukan perancangan topologi untuk merancang jaringan pada sistem On-Grid, maka langkah selanjutnya adalah merealisasikan rancangan topologi tersebut kedalam bentuk *hardware* langsung. Yang digunakan adalah 2 mikrotik sebagai *router* dan juga sebagai *DHCP Server* agar perangkat *monitoring* dan server mendapatkan IP, satu buah *Wireless Extender* yang berfungsi sebagai penangkap sinyal WIFI dari *mobile hotspot* untuk menutupi kelemahan dari salah satu mikrotik yang digunakan, juga digunakan *mobile hotspot* yang berfungsi sebagai simulasi jaringan internet. Setelah semua komponen tersebut dihubungkan, maka akan diuji kestabilan dari jaringan VPN yang sudah dibuat. Jika kedua hal diatas sudah diketahui, maka langkah selanjutnya adalah memasukkan parameter-parameter QOS kedalam *wireshark* untuk melakukan pengujian terhadap jaringan VPN yang telah dibuat sebelumnya. Parameter-parameter QOS yang akan diuji berupa delay, *packet loss,throughput*.

Pada proses tersebut akan diadakan sebanyak dua kali skenario pengujian dimana rincian tentang skenario tersebut adalah sebagai berikut :

1. Menguji penggunaan *tunnel*

   Tunnel atau terowongan adalah salah satu hal yang penting didalam jaringan VPN, karena didalam *tunnel* inilah jaringan yang dibuat dapat mempersingkat jalur *routing*, hal ini menyebabkan data sampai ke tujuan lebih cepat dan menghemat *bandwidth*. Pengujian ini dilakukan karena penggunaan *tunnel* sangat berpengaruh pada kondisi jaringan internet pada saat diuji coba, sehingga untuk mendapatkan data yang lebih valid, proses pengujian penggunaan tunnel dilakukan sebanyak 3 kali yaitu pada saat siang hari, malam hari dan juga pagi hari. Didalam proses menguji penggunaan tunnel perintah yang digunakan di *command prompt* yaitu *command* tracert, *command* ini berfungsi untuk mencatat jalur *routing* yang dipakai

untuk mengirimkan suatu data dari satu ip ke ip yang lain, Dan juga menggunakan aplikasi *wireshark* untuk mencatat delay dan throughput. Pengujian ini dikatakan berhasil apabila dalam proses pengiriman data akan melewati ip *tunnel* yang sudah dibuat dan berdasarkan Parameter yang dipakai yaitu *packet loss* untuk mengetahui berapa paket yang hilang, throughput untuk mengetahui kecepatan pengiriman data, dan juga *delay* untuk menentukan waktu tunda suatu data yang dikirim. Didalam pengujiannya standarisasi yang digunakan adalah ITU-T G.114

2. Menguji *Quality of Service* (QOS) jaringan vpn secara keseluruhan

   Dalam tahap ini dilakukan proses pengujian kualitas layanan, hal-hal yang menjadi parameter pengujian adalah *delay* dan *throughput. D*alam jaringan vpn secara keseluruhan dimana standarisasi yang digunakan dari ITU-T G.114. Didalam pengujian ini menggunakan software *wireshark* dengan memfilter *protocol* ICMP sebagai bahan pengujian, dan dilakukan 3 kali yaitu pada saat malah hari,siang hari dan juga pagi hari untuk melihat stabil atau tidak jaringan yang sudah dibuat.

3. Implementasi On-Grid

   Dalam tahap ini dilakukan proses pengujian yang menghasilkan berhasil atau tidak jaringan yang dibuat untuk memenuhi kebutuhan dari sistem *on-grid* yang sudah dibuat. Indikator keberhasilan dari skenario ini adalah alat *monitoring* harus dapat terkoneksi dengan baik, dan juga mendapatkan ip dari DHCP server yang telah dibuat didalam router. Lalu setelah alat *monitoring* mendapatkan ip dan dapat mengirimkan data, terdapat pemberitahuan "*connected*" diserial arduino. Setelah itu data akan sampai kedalam server yang juga telah dihubungkan kedalam jaringan. Dan jika berhasil maka dari tabel yang telah dibuat di server akan berisi besar tegangan,arus dan frekuensi hasil dari pemonitoran dari alat elektronik yang diukur.

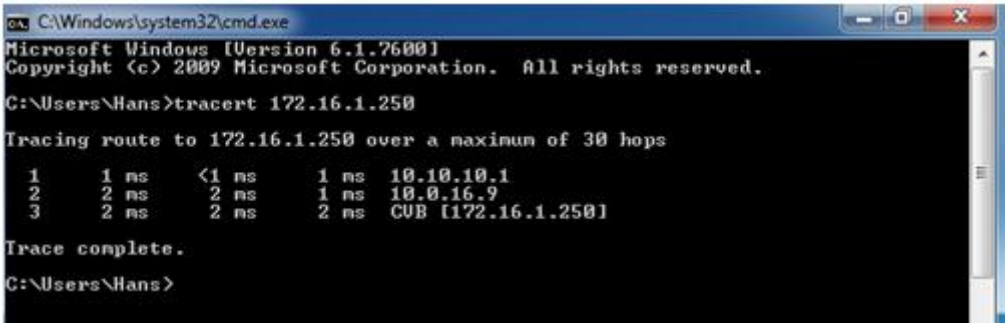
BAB IV

PENGUJIAN DAN IMPLEMENTASI SISTEM

4.1 Hasil Pengujian

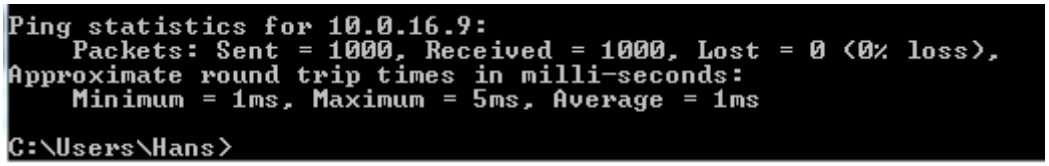
Berikut ini adalah hasil pengujian dari topologi yang sudah direalisasikan untuk jaringan *on-grid*

4.1.1 *Menguji Penggunaan Tunnel*



Gambar 4.1 Hasil *trace route* perangkat *monitoring*-server

Gambar 4.1 adalah hasil dari *trace route* jaringan yang di buat. Trace route adalah metode untuk mengetahui data yang dikirim melewati berapa jalur untuk sampai ke tempat yang dituju. Dari hasil diatas, data dari perangkat *monitoring* yang ber ip 10.10.10.9 dikirimkan melewati *router* dengan ip 10.10.10.1 dan setelah itu data akan dikirimkan ke *tunnel* dengan ip 10.0.16.9. Lalu dari 10.0.16.9 akan dikirimkan ke ip server dengan ip 172.16.1.250.



Gambar 4.2 Hasil uji performansi *tunneling*

Gambar 4.2 adalah hasil dari uji performansi perangkat *monitoring* menuju *tunnel*, hal ini dilakukan untuk mengetahui kestabilan dari hasil topologi dari perangkat *monitoring* menuju *tunnel*. Dari gambar tersebut dilakukan uji coba pengiriman data sebanyak 1000 kali dimana pengujian dilakukan pada siang hari,malam hari dan pagi

hari. Data diatas adalah data ketika uji performansi dilakukan pada malam hari dan hasil yang didapatkan dari uji performansi tersebut adalah data yang diterima sebanyak 1000 buah dan 0 paket data hilang, dengan delay minimum sebesar 1ms dan delay maksimum sebesar 5ms. Untuk hasil performansi pada pagi hari dan siang hari dapat dilihat di lampiran A.

Tabel 4.1 perbandingan uji *tunnel*

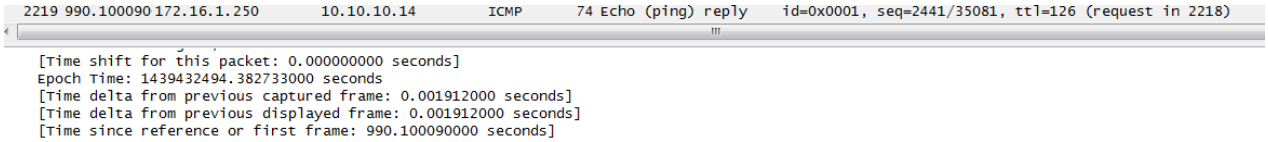
Waktu	Pagi	Siang	Malam	Standarisasi ITu-T
Throughput	0.002 Mb/*second*	0.001 Mb/*sec*	0.002 Mb/sec	Baik
Delay rata-rata	0.002317 *sec*	0.001579 *sec*	0.001886	Baik
Packet Loss	0%	0%	0%	Baik

4.1.2 Menguji Quality of Service (QOS) jaringan vpn secara keseluruhan

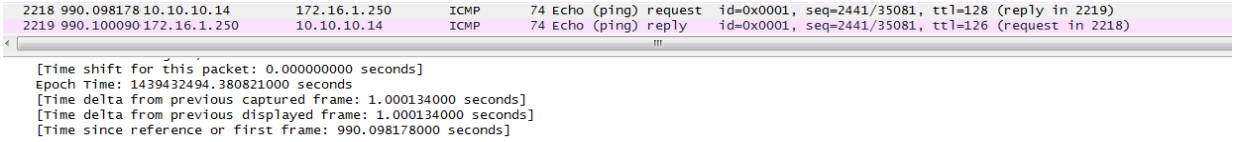
Setelah jalur topologi yang bangun sudah sesuai dengan yang diinginkan, maka langkah selanjutnya yaitu mencari hasil QOS dari jaringan yang dibuat. Pada gambar dibawah ini akan ditampilkan hasil dari pengukuran QOS yang dilakukan pada saat pagi hari

Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	2232	1971	88.306%	0	0.000%
Between first and last packet	1163.227 sec	990.100 sec			
Avg. packets/sec	1.919	1.991			
Avg. packet size	80 bytes	74 bytes			
Bytes	177583	145854	82.133%	0	0.000%
Avg. bytes/sec	152.664	147.312			
Avg. MBit/sec	0.001	0.001			

Gambar 4.3 Hasil throughput



Gambar 4.4 Hasil *reply* delay

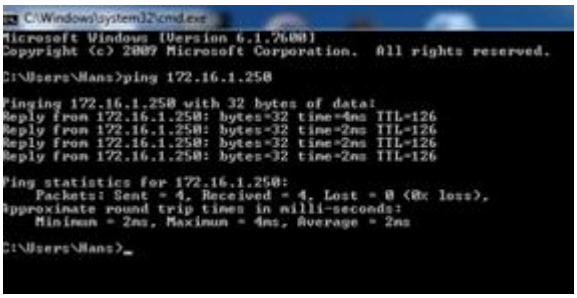


Gambar 4.5 Hasil Request delay

Delay = Paket hasil *reply* – Paket hasil *request*

= 990.100090000 - 990.098178000

= 0.01912



Gambar 4.6 Hasil packet loss

Berikut tabel perbandingan QOS pada pagi siang dan malam hari

Tabel 4.2 Perbandingan performansi QOS

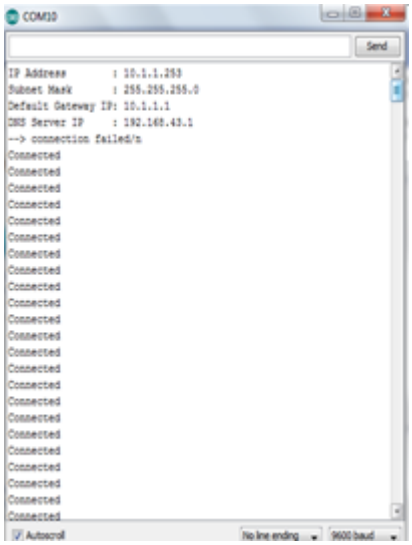
Waktu	Pagi	Siang	Malam	Standarisasi ITU-T
Throughput	0.002 Mb/*sec*	0.001 Mb/*sec*	0.002 Mb/sec	Baik
Delay rata-rata	0.01912 *sec*	0.00261 *sec*	0.002587	Baik
Packet Loss	0%	0%	0%	Baik

4.2 Implementasi *On-Grid*

Setelah topologi jaringan berhasil dibuat dan hasil dari pengukuran QOS baik maka selanjutnya adalah pengimplementasian jaringan dengan perangkat *monitoring* dan server yang sudah dibuat.

Gambar 4.7 Tampilan dis*erver* setelah menerima data

Gambar 4.7 adalah hasil dari penggabungan antara jaringan yang sudah dibangun dengann server yang sudah dibuat. Didalam tampilan dapat dilihat bahwa tegangan dan arus berisi angka-angka, angka-angka itu berasal dari perangkat *monitoring* yang sudah sampai kedalam server. Dan dari angka-angka ini yang nanti akan ditampilkan ke *user.*



Gambar 4.8 hasil di perangkat *monitoring*

Gambar 4.8 adalah tampilan dari perangkat monitoring yang sudah dihubungkan dengan jaringan yang buat dengan topologi yang sudah di gambarkan di bab-bab sebelumnya. Di *interface* arduino perangkat *monitoring* mendapatkan ip 10.1.1.250, ip ini didapatkan dari router yang berfungsi sebagai DHCP *server*. Lalu status *connected* menandakan bahwa perangkat *monitoring* sudah terhubung dengan jaringan dan sedang melakukan proses pengiriman data.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil perancangan, pengujian, hingga analisa maka dapat disimpulkan bahwa:

1. VPN adalah salah satu jalan untuk membangun sistem jaringan untuk On-Grid dikarenakan cukup aman dalam hal hak akses, hal ini dibuktikan dengan jika tidak memiliki hak akses maka data tidak akan dapat terkirim.

2. Dari tiga kali percobaan yang sudah dilakukan sebanyak 1000 kali pengiriman diambil dari pagi,siang dan malam hari maka dapat disimpulkan bahwa delay,throughput bervariatif tetapi masih memenuhi syarat jaringan yang baik menurut standarisasi dari ITU-T yaitu throughput antara 0.01-0.05, delay antara 0.02-0.01 dan memiliki packet loss sebesar 0%.

5.2 Saran

Untuk pengembangan dalam merancang dan mengimplementasikan jaringan ini selanjutnya ada baiknya mempertimbangkan beberapa saran di bawah ini agar didapat hasil yang maksimal :

1. Untuk koneksi internet diharapkan untuk memakai koneksi selain *mobile hotspot* karena *mobile hotspot* tidak stabil

2.Dengan variasi alat dan kelengkapan ip publik, jaringan yang dibentuk akan lebih terlihat *real*

3.Dapat dibuatkan aplikasi yang berfungsi sebagai *monitoring traffic* agar lebih mudah dalam pengontrolan jaringan.

4. Dapat dibuatkan aplikasi menghitung jumlah kapasitas *client* dalam jaringan