Disain Sistem SCADA Jarak Jauh Menggunakan Layanan VPN 3G untuk Penggerak Pompa pada Sistem Pengolahan Air

Remote SCADA System Design Using VPN 3G Services to Drive Pumps in Water Treatment System

Asep Insani dan Sutrisno Salomo H

Bidang Instrumentasi Puslit KIM-LIPI
Kompleks Puspiptek Serpong gedung 420 Tangerang
asepinsani@kim.lipi.go.id,salomo@kim.lipi.go.id

Naskah diterima: 16 Januari 2013; Direvisi: 21 Februari 2013; Disetujui: 1 Maret 2013

Abstract— **In the peat water treatment into clean water using AOP method and the RO, the pump pressure setting is something very vital at the time of supply of water that will be processed into the system. Water treatment systems that use the pump must always be ensured to operate normally adjusted with the designation. Recent management of water treatment systems require the latest technology in equipment remote control system, and the most fundamental of these is the use of public services for the acquisition and control of data taken from the control equipment. To realize remote control for pumps with certain pressure with PLC, is designed with a combination of internet, architecture and implementation of the SCADA system, which combines computer network, PLC, WinCC, and VPN technology. In doing the design, keep in mind the key points of both the server side and the controller. Remote SCADA system design can minimize the time for the operator and further monitoring for water supply.**

***Keywords*— PLC, SCADA remote, VPN.**

Abstrak— **Dalam pengolahan air gambut menjadi air bersih yang menggunakan metode AOP dan RO ini, pengaturan tekanan pompa merupakan sesuatu yang sangat vital pada saat dilakukan suplay air yang akan diolah ke sistem. Sistem pengolahan air yang menggunakan pompa tersebut harus selalu dipastikan beroperasi dengan normal disesuaikan dengan peruntukannya. Manajemen terbaru sistem pengolahan air memerlukan teknologi yang terbaru pada peralatan remote control system, dan yang paling fundamental untuk hal ini adalah penggunaan layanan public untuk akusisi dan pengawasan dari data yang diambil dari peralatan kontrol. Untuk mewujudkan remote control untuk pompa dengan tekanan tertentu dengan PLC, didisain dengan kombinasi antara internet, arsitektur dan implementasi dari sistem SCADA, yang menggabungkan jaringan komputer, PLC, WinCC, dan teknologi VPN. Dalam melakukan disain, perlu diperhatikan poin-poin penting baik dari sisi server maupun sisi controller. Disain sistem SCADA remote dapat mengefisienkan waktu bagi operator dan pemantauan lebih lanjut untuk suplay air.**

***Keywords*— PLC, SCADA remote, VPN**

I. PENDAHULUAN

Information Technology (IT) atau teknologi informasi adalah sebagai studi, desain, pengembangan, implementasi, dukungan terhadap manajemen dari sistem informasi berbasis komputer. Dewasa ini perkembangan alat-alat yang mendukung *Information Technology* (IT) sangat banyak. Beberapa diantaranya adalah berbentuk *website*, teknologi SMS (*short massage service*),dan *streaming video*. Alat-alat tersebut sangat familiar di kalangan masyarakat umum, karena memberikan manfaat untuk menukar informasi dan membuat suatu sistem informasi yangdibutuhkan. Sistem Informasi merupakan komponen-komponen yang saling berhubungan dan bekerjasama untuk mengumpulkan, memproses, menyimpan dan mendistribusikan informasi tersebut untuk mendukung proses pengambilan keputusan, koordinasi dan pengendalian. Sistem informasi dapat diimplementasikan dalam berbagai macam bentuk, salah satunya adalah SCADA(*Supervisory Control And Data Acquisition*).

Komputasi terdistribusi *client/server*, pengaksesan jarak jauh (*remote access*) dan konektifitas antar jaringan telah banyak berperan penting dalam meningkatkan produktivitas

bagi perusahaan dan pegawainya dibandingkan sebelumnya. Pada saat yang bersamaan, perusahaan terus mencari solusi jaringan dan infrastruktur komunikasi data yang fleksibel untuk perkembangan bisnisnya. Teknologi Informasi tidak lagi digunakan sebagai tools atau alat bantu tapi saat ini telah menjadi senjata utama untuk bersaing dan mendapatkan informasi yang update atau terbaru agar keputusan bisnis dapat dengan cepat diambil. Dengan banyaknya solusi-solusi dari vendor-vendor perangkat lunak seperti Oracle, SAP, JDEdward, Microsoft net, dan sebagainya, untuk solusi sistem informasi yang mengintegrasikan semua terminal komputer pegawainya baik yang berada di kantor atau yang *mobile/telecommuters* ke *database* utamanya, memerlukan konektifitas jaringan tulang punggung (*backbone*) yang handal. WAN atau jaringan skala luas yang menjadi solusi untuk infrastruktur komunikasi data tersebut. Dimana da banyak solusi dari teknologi WAN tersebut baik yang berbasis *Circuit Switching* atau *Packet Switching* yang ditawarkan oleh para penyedia jasa telekomunikasi (telco). Sebut saja solusi *Very Small Apperture Terminal* (VSAT), *Leased Channel* (LC), ADSL, *Multi Protocol Labeling Switching* (MPLS), *Frame Relay* dan sebagainya yang merupakan solusi yang ditawarkan telco. Di Indonesia ada banyak provider telco besar yang menawarkan solusi WAN untuk coverage wilayah indonesia, sebut saja TELKOM dengan DynaAccessnya, Indosat dengan Metro-e nya, XL dengan *Business Solutions*, dan Lintas Arta dengan solusi network datanya.

Seperti apa yang telah dipaparkan diatas, maka seiring dengan semakin berkembangnya teknologi informasi yang se,akin cepat dan pesat, maka tuntutan kebutuhan akan informasi semakin meningkat pula. Dimana setiap orang membutuhkan informasi dalam waktu yang cepat, singkat dan akurat oleh karena itu dibutuhkan suatu sarana yang dapat mendukung hal tersebut. Salah satunya adalah koneksi internet yang cepat dan stabil. Sebuah cara harus di temukan untuk mengamankan sebuah jaringan publik tanpa harus melanggar sifat-sifat yang telah ada. Sesungguhnya sebuah jawaban yang ideal harus menyediakan tidak saja tingkat keamanan yang tinggi tetapi juga keamanan yang sedemikian rupa sehingga pengguna dapat dengan mudah mengakses, mengubah dan berbagi lebih banyak informasi, tidak lupa, dibawah kondisi-kondisi yang secara hati-hati dikendalikan dan di pelihara.VPN muncul untuk mengatasi permasalahan tersebut.

Secara umum, VPN (*virtual private network*) merupakan sebuah proses dimana jaringan umum (*public network* atau internet) diamankan untuk memfungsikannya sebagaimana jarigan privat (*private network*). Sebuah VPN tidak didefinisikan oleh rangkaian khusus atau *router*, tetapi didefinisikan oleh mekanisme keamanan dan prosedur-prosedur yang hanya mengijinkan penggunanya yang ditunjuk akses ke VPN dan informasi yang mengalir melaluinya.

Kecepatan akses internet yang semakin cepat dan meningkatnya trafik membuat internet menjadi hal yang penting dalam dunia komunikasi.untuk menjaga agar kompetitif kestabilan akses, *network operator* atau *internet service provider* yang memang berhubungan dengan komunikasi data, harus menambah *backbone trafic* yang kontinyu dan menyediakan kualitas layanan atau *Quality of service* (Qos) yang bagus untuk trafik jaringan.

Suatu jaringan dapat di katakan trafiknya padat atau tinggi apabila banyak *host* yang melakukan koneksi ke server dalam jaringan tersebut, sehingga lalu lintas paket data padat dalam jaringan. masalah yang mempengaruhi kinerja jaringan komputer di antaranya adalah *bandwith,latency* dan jitter.yang membuat efek yang cukup besar bagi aplikasi dalam suatu jaringan.

Kemanan pengiriman data dan perhitungan kecepatan akses yang menghasilkan kualitas sangat baik, merupakan implementasi dari *Virtual Private network*. Dalam sistem pengolahan air, tekanan pompa dengan pengaturan tertentu merupakan bagian yang paling penting, dan dibutuhkan waktu mapuan pengoperasian sistem untuk memantau dan mepertahankan keadaan sistem dengan operasi yang terpantau. Otomatisasi proses untuk malakukan pemompaan dapat meningkatkan kinerja secara keseluruhan. Dalam beberapa tahun terakhir ini, otomasi indudtri tidak lagi dibatasi jarak antara stasiun operator pengontrol dan terminal control. Selain itu PLC generasi terbaru mendukung hal ini dengan kemampuan yang dimilikinya untuk akusisi data melalui VPN berbasis 3G untuk menetukan kondisi terminal kontrol atau memeriksa statusnya. Sistem kontrol modern untuk instalasi pengolahan air tidak hanya dirancang untuk memenuhi kebutuhan umum dari proses ini, tetapi juga harus mudah untuk diintegrasikan ke dalam berbagai arsitektur, termasuk jaringan publik.

Seiring dengan berkembangnya VPN (*Virtual Private Network*), serta adanya fleksibilitas koneksi VPN yang bisa dilakukan secara *private*, maka ini sangat membantu sekali untuk menangani jaringan koneksi untuk bidang proses kontrol industri, *remote* diagnostik, dan pemeliharaan *remote* peralatan kontrol industri, dan hal itu semua merupakan bagian dari teknologi otomatisasi saat ini. Koneksi dengan menggunakan *remote* dari peralatan kontrol memberikan penghematan besar baik dalam waktu maupun biaya, dalam hal ini erat kaitannya dengan industri. Oleh karena itu sistem pengendali dengan remote peralatan instrumentasi,dalam hal ini untuk pengendalian pompa dengan tekanan tertentu dapat diapliksikan dengan teknologi VPN berbasis 3G.

Implementasi yang dilakukan untuk sistem pengontrol pada pengolahan air gambut menjadi air bersih dengan metode AOP dan RO menggunakan PLC sebagai kontroler. PLC ini modul I/O yang dimilikinya memiliki keterbatasan jarak dari divais yang dikontrol ke PLC, jarak aman pengkabelan dari sistem ke modul I/O PLC adalah sejauh 20 meter, lebih dari jarak tersebut,maka sistem akan mengalami gangguan terutama untuk modul I/O PLC. Sedangkan untuk analog I/O pada jarak 30 meter masih memungkinkan, hal ini dikarenakan sinyal yang dikirim adalah arus untuk I/O analog sedangkan untuk I/O digital berupa tegangan. Sehingga untuk digital, jika jarak divais yang dikontrol lebih dari 20 meter, maka diperlukan beberapa PLC. Pengembangan lebih lanjut untuk sistem kontrol PLC ini digunakan koneksi jaringan 3G dengan metode *Virtual Private Network*. Dalam paper ini, akan di sajikan tentang disain arsitektur jaringan 3G dengan VPN untuk memantau tekanan pompa motor pada proses kontrol pengolahan air gambut menjadi air bersih.

II. TINJAUAN PUSTAKA

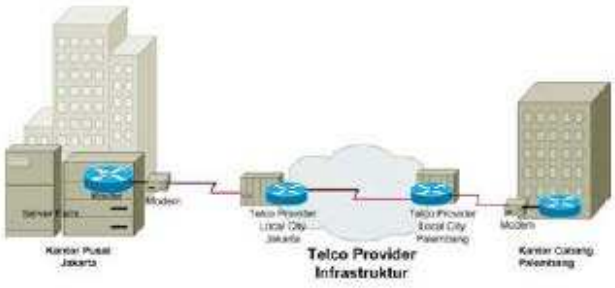
A. Jaringan Komunikasi Data WAN

Ada banyak solusi yang bisa digunakan untuk komunikasi data pada jaringan skala luas, saat ini terdapat beberapa solusi komunikasi data yang ditawarkan oleh *telco provider*. WAN adalah jaringan komunikasi yang meliputi area geograpis yang luas dan biasanya menggunakan fasilitas dari transmisi provider, seperti perusahaan telpon atau lainnya (Marilee Ford, dkk, *Internetworking Techlogies Handbook*, 1997 : 45). Dalam jaringan WAN sangat *sensitive* dengan masalah lebar pita (*bandwidth*), para penyedia jasa biasanya menentukan biaya sewa dari layanan dan bandwidth yang digunakan. Ada beberapa layanan WAN y ang sering menjadi ukuran layanan perusahaan telekomunikasi terhadap pelanggannya.

TABEL 1. LAYANAN WAN DAN *BANDWIDTH*

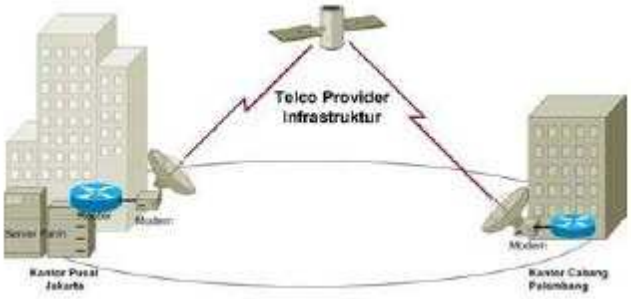
Layanan	Type User	Bandwidth
T1	*Larger Entities*	1,544 Mbps
E1	*Larger Entities*	2,048 Mbps
T3	*Larger Entities*	44,736 Mbps
E3	*Provider backbone* Telekomunikasi	34,368 Mbps
STS-A (OC-1)	*Provider backbone* Telekomunikasi	51.840 Mbps
STM-1	*Provider backbone* Telekomunikasi	155,52 Mbps
STS-3 (OC-3)	*Provider backbone* Telekomunikasi	155,251 Mbps
STM-3	*Provider backbone* Telekomunikasi	466,56 Mbps
STS-48 (OC-48)	*Provider backbone* Telekomunikasi	2,488320 Gbps

Leased Channel, solusi untuk mengkoneksikan jaringan kita dengan menyewa pada operator telekomunikasi untuk *bandwidth* tertentu, biasanya biaya dihitung dari banyaknya node, besarnya *bandwidth* yang digunakan dan jarak antara node tersebut, semakin besar bandwidth dan semakin jauh jarak antara satu *node* dengan yang lain akan semakin mahal biayanya. Perusahaan telekomunikasi yang kita sewa biasanya perusahaan yang telah mempunyai infrastruktur ke seluruh Indonesia atau keluar negeri (tergantung kebutuhan), infrastruktur kebanyakan menggunakan Teresterial dan Metro-e yang rata-rata *backbonenya* menggunakan Fiber Optic (FO).



Gambar 1. Solusi Leased Channel Pada Jaringan Skala Luas (WAN)

VSAT (*Very Small Aperture Terminal*), komunikasi yang menggunakan media *satellite* diluar muka bumi sebagai *transmitter* dan *receiver*-nya dari tempat yang berada di permukaan bumi ke tempat lain selama masih dalam *coverage area* (*hotspot area*) dari satelit tersebut. Solusi ini sering digunakan perusahaan minyak lepas pantai, kehutanan jauh didalam hutan, riset di pegunungan atau gurun, yang jauh dari *coverage* area layanan. Namun VSAT biasanya digunakan sebagai solusi terakhir jika layanan lain tidak tersedia dikarenakan *latency* yang besar dan sangat rentan terhadap gejala alam, VSAT sangat tidak sesuai untuk solusi komunikasi data dan suara yang memerlukan kualitas yang prima dan *reliable*.



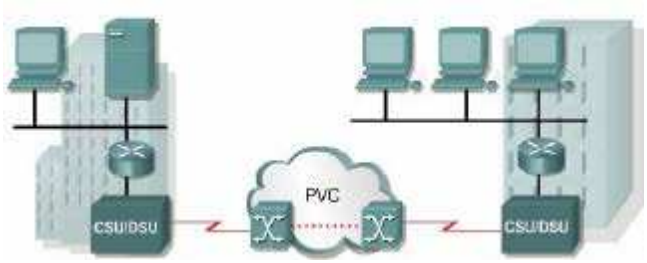
Gambar 2. Solusi VSAT Pada Jaringan Skala Luas (WAN)

DSL (*Digital Subscriber Line*), DSL sering menjadi solusi telko untuk menghubungkan ke *end user*. Ada banyak varian DSL yang sering disebut XDSL (ADSL, SDSL, VDSL, dan lain-lain). *Asymmetric DSL* yang paling banyak saat ini digunakan karena versi ekonomis dari DSL, teknologi ini memungkinkan transfer data download bisa tinggi namun berbeda dengan uploadnya yang transfernya lebih kecil dari download. ADSL adalah teknologi yang menggunakan jaringan line telpon *twister-pair* yang ada untuk mengalirkan data dengan kecepatan tinggi seperti multimedia dan video.

Keuntungan lainnya adalah ADSL bisa menggunakan *fixed cable* yang *existing* seperti PSTN salah satu telco tanpa menggangu komunikasi suara. Namun kelemahannya adalah jarak yang pendek, rata-rata berjalan dengan baik dibawah jarak 5 km. Saat ini ada teknologi VPN yang banyak ditawarkan *telecommunication provider* yang merupakan solusi hemat yang banyak digunakan perusahaan untuk *mengkoneksikan* cabang / mobile user ke server pusatnya.

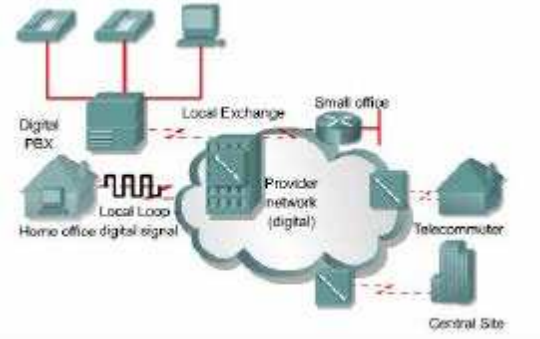
Frame Relay, suatu skema teknologi WAN yang dibuat untuk memperbaiki dari teknologi X.25. *Frame Relay* menjadi pilihan utama dahulu karena jaringan ini dapat diimplementasikan dengan interkoneksi perangkat pasaran. *Frame Relay* dirancang berdasarkan konsep *Virtual Circuit* (VC), VC merupakan sebuah jalur sambungan dua arah didalam jaringan yang didefinisikan oleh *software.* Frame relay dapat dapat menangani error dan pengelamatan di jaringan, namun sangat rentan terhadap ganggunan pengiriman paket data (drop) dan keterlambatan (delay) karena *Frame Relay* tidak dapat memilah paket yang lewat di jaringan, hal ini sangat tidak diinginkan dengan kondisi pengiriman data saat ini yang menginginkan jaringan yang reliable dan stabil. **ISDN** atau *Integrated System Digital Network* dirancang untuk membawa data, suara dan Video. Teknologi yang memungkinkan membawa data digital pada

kabel analog dengan membawa data lebih besar dan proses koneksi lebih cepat dari *dial-up* biasa. ISDN menjadi trend pada era tahun 90an dikarenakan teknologi yang bisa membawa paket data dengan kecepatan yang tinggi namun dahulu cocok dengan infrastruktur *last miles* di indonesia.



Gambar 3. Solusi frame Relay Jaringan Skala Luas

ISDN menyediakan dua tingkatan pelayanan, *Basic Rate Interface* (BRI) dan *Primary Rate Interface* (PRI)



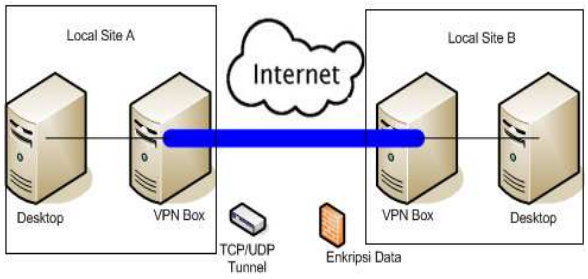
Gambar 4. Solusi ISDN Jaringan Secara Luas

B. Layanan VPN 3G

VPN merupakan singkatan dari *Virtual Private Network* yang artinya membuat jaringan private secara virtual diatas jaringan *public*(umum) seperti internet. VPN berkembang dikarenakan adanya perkembangan yang pesat pada perusahaan-perusahaan besar yang ingin tetap memperluas jaringan bisnisnya, namun mereka tetap ingin terhubung ke jaringan local(private) mereka dengan kantor cabang yang dimiliki dan perusahaan mitra kerjanya yang berada di tempat yang jauh. Perusahaan juga ingin memberikan hak akses kepada pegawai khusus sebagai fasilitas yang efektif dan efisien agar dapat terhubung ke jaringan lokal milik perusahaan tersebut di manapun mereka berada. Perusahaan tersebut perlu suatu jaringan lokal yang jangkauannya luas, tidak bisa diakses oleh sembarang orang, tetapi hanya orang yang memiliki hak akses saja yang dapat terhubung ke jaringan lokal tersebut sehingga keamanan perusahaan dapat terjaga. Implementasi jaringan tersebut dapat dilakukan dengan menggunakan *leased line*(jalur penyewaan). Namun biaya yang dibutuhkan untuk membangun jaringan yang luas menggunakan leased line sangat besar. Di sisi lain perusahaan juga ingin mengoptimalkan biaya untuk membangun jaringan mereka 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 public yang sudah ada, misal : internet.

VPN dapat diartikan sebagai suatu jaringan private yang mempergunakan sarana jaringan komunikasi public yaitu Internet dengan memakai tunelling protokol dan prosedur pengamanannya.

VPN 3G merupakan salah satu solusi layanan telekomunikasi untuk memenuhi spesifikasi dan memungkinkan penggunaan secara simultan dari layanan suara dan data dengan kecepatan data yang lebih tinggi jika dibandingkan dengan generasi yang sebelumnya yaitu GPRS. Dalam beberapa tahun terakhir ini, jaringan wireless dengan pengaturan bandwidth,mulai melakukan ujicoba praktis dengan penerapan VPN 3G untuk aplikasinya. Dilain pihak penggunaan 3G sendiri untuk layanan data sudah mulaim menurun, seiring dengan meluasnya layanan 3G VPN. Sistem SCADA dengan menggunakan *remote* VPN dengan teknologi berbasis 3G, yang bekerja dengan menghubungkan antara komputer dan router nirkabel melalui jaingan lokalatau wide area dilakukan dengan enkapsulasi program untuk privasi data agar data tetap aman. Selama dilakukannya pembangunan VPN, router kabel yang terhubung dengan sinyal jaringan PLC ke komputer di stasiun pengontrol, bertujuan untuk mengatur tunneling antara komputer atas dan router nirkabel industri. Dan *Virtual Private Network* adalah perpaduan dari teknologi tunelling dengan teknologi enkripsi. Kedua teknologi tersebut saling melengkapi.



Gambar 5. *Virtual Private Network* (VPN)

VPN harus mampu menyediakan tiga fungsi utama untuk penggunaannya. Ketiga fungsi tersebut adalah sebagai berikut:

1. *Confidentially* (kerahasiaan)

Dengan digunakannya jaringan public yang rawan pencurian data,maka teknologi VPN menggunakan sistem kerja dengan cara mengenkripsi semua data yang melewatinya. Dengan adanya teknologi enkripsi tersebut, maka kerahasiaan data dapat lebih terjaga. Walaupun ada pihak yang dapat menyadap data yang melalui internet, bahkan melalui jalur VPN itu sendiri. Namun belum tentu dapat membaca data tersebut,karena data tersebut telah teracak.

2. *Data Integrity* (keutuhan data)

Ketika melewati jaringan internet, sebenarnya data telah berjalan sangat jauh melintasi berbagai Negara. Pada saat perjalanan tersebut, berbagai gangguan dapat terjadi terhadap isinya. Baik hilang, rusak,ataupun dimanipulasi oleh orang yang tidak seharusnya.Pada VPN, terdapat teknologi yang dapat menjaga keutuhan data mulai dari data yang dikirim hingga data sampai di tempat tujuan.

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 dari sumber datanya. Kemudian alamat sumber data tersebut, akan disetujui apanbila proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya. Tidak ada data yang dipalsukan atau dikirim oleh pihak-pihak lain.

Pembangunan aplikasi sistem informasi sistem VPN disusun dengan maksud dan tujuan yaitu:

1. 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.
2. Bisa 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, General Ledger, Remote Web Camera, Aplikasi SCADA untuk sistem pemantau, dan lain-lain.
3. Operator pada sistem pengontrol dengan cepat & tepat mengambil keputusan yang akan diambil, karena operator tersebut dimanapun bisa mengakses sistem yang terhubung dengan internet karena master unit yang berupa laptop terhubung langsung ke sistem database melalui koneksi VPN server.
4. Mensupport unlimited jumlah server & client yang berada dibelakang router server secara simultant.
5. Dimanapun berada dapat melakukan koneksitas dengan PC dikantor misalnya dengan memanfaatkan software yang bekerja dijaringan LAN seperti Citrix, Windows Terminal Server, VNC, Radmin, VOIP, dan lain sebagainya.
6. Penggunaaan VPN dapat mengurangi biaya operasional bila dibandingkan dengan penggunaan leased line sebagai cara tradisional untuk mengimplementasikan WAN.
7. 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.
8. Menggunakan internet sebagai media komunikasinya. Pengguna VPN hanya membutuhkan biaya dalam jumlah yang relatif kecil untuk menghubungkan perusahaan tersebut dengan pihak ISP (internet service provider) terdekat.
9. Memberi kemudahan untuk diakses dari mana saja, sehingga suatu sistem / peralatan yang mobile dapat mengakses jaringan khusus perusahaan di manapun berada. Selama bisa mendapatkan akses internet ke ISP terdekat, operator pada sistem pengontrol tetap dapat melakukan koneksi dengan jaringan khusus.

Beberapa keunggulan menggunakan VPN sebagai pembanding jaringan skala luas (WAN) yang membuat banyak telco provider menawarkan solusi ini dan banyak perusahaan mulai beralih ke teknologi tersebut, beberapa keunggulannya adalah ;

1. Standarisasi, kompatibel dengan standarstandar protocol *Internet Engineering Task Force* (IETF) dan vendor dunia lainnya.
2. Lebih ekonomis, lebih murah dibandingkan dengan solusi lain karena interkoneksi dilewatkan di jaringan Internet dan tidak memerlukan perangkat khusus jika infrastruktur yang telah ada mendukung jaringan VPN.
3. Biaya sewa link yang murah dari penyedia jasa backbone dikarenakan menggunakan layanan jaringan baru yang lebih ekonomis seperti *MultiProtocol Labeling Switching* (MPLS).
4. Fleksibel Arsitektur, dapat dikoneksikan dengan infrastruktur yang sudah ada seperti peralatan router/swtich yang mendukung VPN.
5. Integrasi Konektifitas Multimedia yang tinggi, akses dimana saja ke global interkoneksi untuk koneksi data, suara, dan video.
6. *Scalability*, memungkinkan penyedia jasa untuk tetap bisa melayani permintaan pasar tanpa harus kehilangan kesempatan.
7. *Security*, memungkinkan traffic kritikal bisnis dengan aman dengan digunakannya metode tunneling dan enkripsi.
8. *Managable*, sangat cocok untuk efektifitas biaya karena kemudahan dalam manajemen vendor untuk multiple service berbasis IP.
9. *Traffic engineering*, mudah dalam pengaturan *traffic bandwidth*, mekanisme *restorasi fault* dan mekanisme proteksi.
10. Fast deployment, cocok untuk perusahaan yang memerlukan aplikasi-aplikasi berbasis IP yang cepat perubahannya.
11. Jaminan *Service Level Aggreament* (SLA) dan Jaminan Kualitas Layanan atau *Quality of Services* (QoS), jaminan layanan *uptime* bagi kebutuhan akan kestabilan interkoneksi dan jaminan yang tinggi atas koneksi dapat dipenuhi dan memungkinkan prioritas berdasarkan kritikan atau traffic yang sensitifitas atas delay.

C. Open VPN

OpenVPN adalah aplikasi *open source* untuk *Virtual Private Networking* (VPN), dimana aplikasi tersebut dapat membuat koneksi *point-to-point tunnel* yang telah terenkripsi. *OpenVPN* merupakan *full-featured* SSL VPN yang mengimplementasikan OSI *layer* 2 dan 3 *network extension* menggunakan standar SSL/TLS protokol, mendukung metode otentikasi klien berdasarkan sertifikat yang fleksibel, *smart card*, dan *username / password* serta memungkinkan pengguna atau kelompok tertentu melakukan akses kontrol terhadap kebijakan (*policies*) menggunakan aturan *firewall* yang diterapkan pada *interface* VPN *virtual*. *OpenVPN* bukan aplikasi *web proxy* dan tidak beroperasi melalui *web browser.*

D. Router

Router adalah perangkat yang akan melewatkan paket IP dari suatu jaringan ```ke jaringan yang lain, menggunakan metode *addressing* dan protokol tertentu untuk melewatkan paket data tersebut. Router memiliki kemampuan melewatkan paket IP dari satu jaringan ke jaringan lain yang mungkin memiliki banyak jalur diantara keduanya.

E. Jaringan Komputer

Jaringan komputer adalah sekumpulan komputer yang terhubung satu dengan lainnya menggunakan protocol komunikasi melalui media komunikasi sehingga dapat menggunakan sumber daya bersama seperti harddisk, printer, dan sumber informasi lainnya Tujuan dibangunnya jaringan computer adalah membawa suatu informasi secara tepat dan tanpa adanya kesalahan dari sisi pengirim menuju sisi penerima melalui media komunikasi.

F. Android

Android adalah sistem operasi untuk telepon seluler yang berbasis *Linux*. *Android* menyediakan *platform* yang bersifat *open source* bagi para pengembang untuk menciptakan sebuah aplikasi.

G. Teknologi Tunelling

Teknologi Tunelling merupakan teknologi yang bertugas untuk menangani dan menyediakan koneksi point to point dari sumber ke tujuannya. Disebut tunnel Karen koneksi point to point tersebut sebenarnya terbentuk dengan melintasi jaringan umum,namun koneksi tersebut tidak memperdulikan paket-paket data milik orang lain yang sama-sama melintasi jaringan umum tersebut, tetapi koneksi tersebut hanya melayani transportasi data dari pembuatannya. Hal ini sama dengan seperti penggunaan jalur busway yang pada dasarnya menggunakan jalan raya, tetapi dia membuat jalur sendiri untuk dapat dilalui bus khusus.

Koneksi point to point ini sesungguhnya tidak benar-benar ada, namun data yang dihantarkannya terlihat seperli benar-benar melewati koneksi pribadi yang bersifat point to point.

Teknologi ini dapat dibuat diatas jaringan dengan pengaturan IP addressing dan IP routing yang sudah matang. Maksudnya, antara sumber tunnel dengan dengan tujuan tunnel telah dapat saling berkomunikasi melalui jaringan dengan pengalamatan IP .

H. Point to Point Tunelling Protocol (PPTP)

PPTP merupakan protokol yang mengizinkan hubungan point to point protocol (PPP) melewati jaringan IP, dengan membuat Virtual Private Network (VPN). Teknologi jaringan PPTP merupakan pengembangan dari remote access Point to Point protocol yang dikeluarkan oleh Internet Engineering Task Force (IETF). PPTP merupakan protokol jaringan yang merubah paket PPP menjadi IP datagrams agar dapat ditransmisikan melalui internet. PPTP juga dapat digunakan pada jaringan private LAN to LAN.

PPTP terdapat sejak dalam sistem operasi windows NT Server dan Windows NT Workstation versi 4.0.Komputer yang berjalan dengan sistem operasi tersebut dapat menggunakan protokol PPTP dengan aman untuk terhubung dengan private network sebagai klien dengan remote access melalui internet. PPTP juga dapat digunakan oleh komputer yang terhubung dengan LAN untuk membuat VPN melalui LAN.

I. *SCADA*

SCADA adalah suatu sistem pengakuisisian suatu data untuk digunakan sebagai control dari sebuah obyek. Sistem SCADA yang paling sederhana yang mungkin bisa dijumpai di dunia adalah sebuah rangkaian tunggal yangmemberitahu anda sebuah kejadian (event). Sebuah sistem SCADA skala-penuh mampu memantaudan (sekaligus) mengontrol proses yang jauh lebih besar dan kompleks.

Sebuah sistem SCADA memiliki 4 (empat) fungsi , yaitu:

1.Akuisisi Data,
2.Komunikasi data jaringan,
3.Penyajian data, dan
4.Kontrol (proses).

Fungsi-fungsi tersebut didukung sepenuhnya melalui 4 (empat) komponen SCADA, yaitu:

1. Sensor (baik yang analog maupun digital) dan relai kontrol yang langsung berhubungandengan berbagai macam aktuator pada sistem yang dikontrol.

2. RTUs (Remote Telemetry Units). Merupakan unit-unit "komputer" kecil (mini),maksudnya sebuah unit yang dilengkapi dengan sistem mandiri seperti sebuah komputer,yang ditempatkan pada lokasi dan tempat-tempat tertentu di lapangan. RTU bertindak sebagai pengumpul data lokal yang mendapatkan datanya dari sensor-sensor danmengirimkan perintah langsung ke peralatan di lapangan.

3.Unit master SCADA (Master Terminal Unit - MTU). Merupakan komputer yangdigunakan sebagai pengolah pusat dari sistem SCADA. Unit master ini menyediakan HMI (Human Machine Iterface) bagi pengguna, dan secara otomatis mengatur sistem sesuaidengan masukan-masukan (dari sensor) yang diterima.

4.Jaringan komunikasi, merupakan medium yang menghubungkan unit master SCADA dengan RTU-RTU di lapangan.

Pada kenyataannya untuk Akuisisi Data, kita membutuhkan pemantauan yang jauh lebih banyak dan kompleksuntuk pengukuran terhadap masukan dan beberapa sensor digunakan untuk pengukuran terhadapkeluaran (tekanan, massa jenis, densitas dan lain sebagainya).Beberapa sensor bisa melakukan pengukuran kejadian secara sederhana yang bisa dideteksimenggunakan saklar ON/OFF, masukan seperti ini disebut sebagai masukan diskrit atau masukan digital

. Misalnya untuk mengetahui apakah sebuah alat sudah bekerja (ON) atau belum (OFF),konveyornya sudah jalan (ON) atau belum (OFF), mesinnya sudah mengaduk (ON) atau belum(OFF), dan lain sebagainya. Beberapa sensor yang lain bisa melakukan pengukuran secarakompleks, dimana angka atau nilai tertentu itu sangat penting, masukan seperti ini disebut masukan analog bisa digunakan untuk mendeteksi perubahan secara kontinu pada: tegangan, arus, densitas cairan, suhu, dan lain sebagainya. Untuk kebanyakan nilai-nilai analog, ada batasan tertentu yang didefinisikan sebelumnya, baik batas atas maupun batas bawah. Misalnya, Anda ingin mempertahankan suhu antara 30 dan 35derajat Celcius, jika suhu ada di bawah atau diatas batasan tersebut, maka akan memicu alarm (baik lampu dan/atau bunyi-nya). Terdapat empat alarm batas untuk sensor analog: Major Under, Minor Under, Minor Over, dan Major Over Alarm.

Untuk melakukan suatu komunikasi data, pada awalnya, SCADA melakukan komunikasi data melalui radio, modem atau jalur kabelserial khusus. Saat ini data-data SCADA dapat disalurkan melalui jaringan Ethernet atau TCP/IP.Untuk alasan keamanan, jaringan komputer untuk SCADA adalah jaringan komputer lokal (LAN -Local Area Network) tanpa harus mengekspos data-data penting di Internet.Komunikasi

SCADA diatur melalui suatu protokol, jika jaman dahulu digunakan protokolkhusus yang sesuai dengan produsen SCADA-nya, sekarang sudah ada beberapa standar protokolyang ditetapkan, sehingga tidak perlu khawatir masalah ketidakcocokan komunikasi lagi.Karena kebanyakan sensor dan relai kontrol hanyalah peralatan listrik yang sederhana, alat-alat tersebut tidak bisa menghasilkan atau menerjemahkan protokol komunikasi. Dengan demikiandibutuhkan RTU yang menjembatani antara sensor dan jaringan SCADA. RTU mengubah masukan-masukan sensor ke format protokol yang bersangkutan dan mengirimkan ke master SCADA, selain itu RTU juga menerima perintah dalam format protokol dan memberikan isinya listrik yang sesuai ke relai kontrol yang bersangkutan dan mengirimkan ke master SCADA, selain itu RTU juga menerima perintah dalam format protokol dan memberikan sinyal listrik yang sesuai ke relai kontrol yang bersangkutan.

Untuk penyajian data, Sistem SCADA melakukan pelaporan status berbagai macam sensor (baik analog maupundigital) melalui sebuah komputer khusus yang sudah dibuatkan HMI-nya (*Human Machine Interface*) atau HCI-nya (*Human Computer Interface*). Akses ke kontrol panel ini bisa dilakukan secara lokal maupun melalui *website*. Bahkan saat ini sudah tersedia panel-panel kontrol yang *Touch Scree*n.

Kita bisa melakukan penambahan kontrol ke dalam sistem SCADA melalui HMI-nya. Bisadilakukan otomasi kontrol atau otomasi proses, tanpa melibatkan campur tangan manusia.

J. Membangun Sistem Scada Remote

Sistem kontrol yang diajukan untuk sistem ini adalah dengan menggunakan PLC Omron CJ2M-CPU31. Untuk menggunakan 3G,kita menggunakan jaringan tertutup dengan LAN, membangun wireless router dengan mengkoenksikan kembali server VPN. Pada satu sisi dari router, ada komputer pada stasiun kontrol,dan pada sisi yang lain.Yang dilakukan untuk membangun sistem ini antara lain:

1. *Setting* IP address sistem. Dilakukan setting *ethernet* untuk sistem yaitu dengan :
2. IP *address wireless router* adalah : 192.168.1.2
3. IP *address* PLC Omron adalah: 192.168.1.11
4. IP *address* pada komputer untuk master kontrol adalah 192.168.1.158.
5. IP *address public network* diberikan oleh *internet service provider.*

K. Membangun VPN Tunelling

VPN Tunelling dibangun dengan komunikasi antara VPN server pada komputer master dan VPN client yang dibangun oleh wireless router. Karena PC Srver VPN berada pada samping *wireless router*, maka *router* harus dikonfigurasi dengan menggunakan akses PPTP VPN.

Pada station master ,IP address dari PC server VPN dialokasikan secara otomatis oleh router secara umum.Untuk menjadikan VPN client berhasil melakukqan koneksi ulang dengan VPN server, harus digunakan fungsi *Network Address Translation* (NAT). yang secara umum merupakan routing network traffic diantara LAN dan WAN.

Untuk melakukan setting PLC untuk menangani komunikasi antara jaringan lokal sebaik menangani pesan dari jaringan secara luas, sebuah alamat *gateway* ditambahkan untuk mengirimkan IP address wireless router ke PLC dan ke static router, untuk IP address PLC ditambahkan dengan menggunakan command ping juga. Dalam hal ini PLC mempunyai kemampuan untuk mengirim dan menerima IP pesan yang tidak dibangun didalam jaringan lokal.

L. Cara Melakukan Setting VPN

Hal-hal yang perlu untuk membuat sebuah server vpn yang via jaringan GSM, CDMA, 3G dari berbagai yang ada adalah sebagai berikut:

1. Di sisi server vpn harus menggunakan IP publik, tujuannya agar client yang berasal dari jaringan internet (GPRS, CDMA, 3G) bisa masuk ke server VPN Master.
2. Server VPN harus di set dengan benar.
3. Server VPN harus bisa akses ke internet, yaitu bisa melakukan koneksi ke internet, dengan melakukan pengesetan: Touting, DNS, NAT, dan sebagainya.
4. Setup disisi client juga harus benar, namun umumnya sama dengan setup koneksi dial up atau speedy. cuma bedanya di pilihan jenis koneksinya dipilih VPN. Dan IP server VPN juga dimasukan dengan benar.

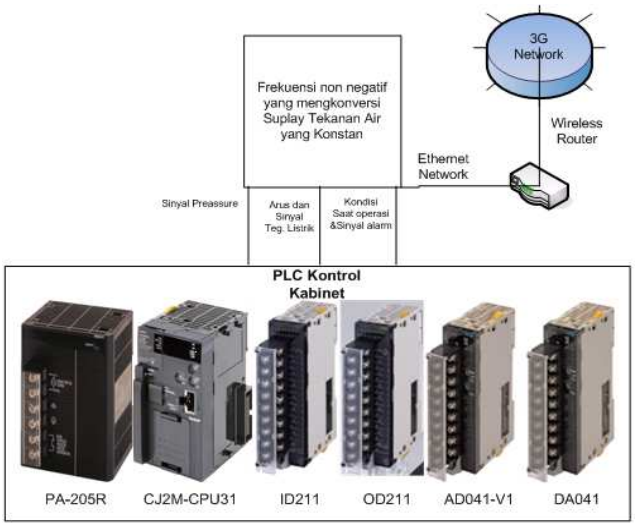
M.Perangkat Keras Sistem

Perangkat PLC yang digunakan untuk sistem SCADA remote adalah PLC Omron CJ2M-CPU31 memiliki kapasitas memori 5 Ksteps dan mempunyai 160 I/O unit. Tipe ini digunakan untuk aplikasi yang sangat sederhana, karena keterbatasan memori. Untuk komunikasi CJ1M-CPU11 ini dengan komputer digunakan komunikasi serial RS-232. Kemudian untuk pemrograman ladder diagramnya digunakan software CX-programmer.

PLC dapat berkomunikasi dengan komputer dengan menggunakan *host link.Host lin*k ini merupakan *interface* PLC terhadap host komputer.Melalui host link, seluruh area memori dalam PLC dapat diakses termasuk memori program. Kabinet kontrol pada PLC ini dilengkapi dengan modul CPU dan modul input analog. Poin masukan dari PLC dihubungkan ke sinyal yang dating dari berbagai komponen (pompa air, katup, dll). Pengiriman data secara real time ini meliputi akusisi dan proses analog juga switch yang diperoleh dari konversi frekuensi tekanan air peralatan secara konstan yang tidak negative. Semua sinyal kontrol, sinyal status, sinyal alarm dan pengolahan variable data akan dikirim dan diterima antara lokasi pusat dan situs remote melalui VPN dengan memanfaatkan 3G. Di bawah ini adalah gambar disain akusisi data.

N. Data Akuisisi Dan Proses

Data real-time termasuk akuisisi dan pengolahan analog dan switch, yang semuanya diperoleh dari konversi frekuensi dari pasokan peralatan tekanan air yang dilakukan dengan konstan. Semua sinyal kontrol, sinyal status, sinyal alarm dan data variabel proses harus dikirimkan dan diterima antara lokasi pusat dan situs remote melalui VPN memanfaatkan 3G. Tingkat tekanan yang berbeda, lalu lintas, data analog sensor tekanan melalui modul akuisisi, aka akan membawa data menuju ke pengolahan data, dan data ini sesuai dengan kisaran kalibrasi sensor. Desain gambar akuisisi data ditunjukkan pada sebagai berikut:



Gambar 6. Disain Data Akusisi

III. METODE PENELITIAN

O. Perancangan Metode Pengujian Vpn 3g

Pertama kali, dilakukan perancangan metode pengujian untuk membandingkan *mobile* VPN menggunakan protokol PPTP dengan jaringan 3G. Perancangan dimulai dengan perencanaan topologi pada jaringan, *software* dan hardware yang digunakan,instalasai dan konfigurasi jaringan *serta* persiapan pengujian.

1. Perencanaan dan Desain Topologi Jaringan

Model topologi yang digunakan pada pengujian kali ini adalah dengan satu buah laptop yang berfungsi sebagai server,ponsel sebagaia klien, Model ADSL yang dikonfigurasi agar bisa dilewatkan data VPN PPTP,akses internet baik *fixed lined* dari sisi server maupun *wireless* dari sisi klien. Pengukuran akan dilakukan dari sisi server.

Server ini dirancang untuk menangani koneksi *remote* ke perangkat *android* menggunakan *OpenVPN Server* yang di instal pada *Linux Ubuntu 12.04.1 LTS 32bit.* Koneksi internet yang digunakan dalam pembuatan *server* ini adalah koneksi Telkom *Speedy. Server* ini berada pada jaringan lokal yang ada di belakang *router* berbasis *Mikrotik RouterOS* yang terhubung ke *internet* dan memiliki *fixed IP address*. *Router* ini dikonfigurasi untuk meneruskan koneksi TCP di *port* 3080 pada IP *external* ke *port* 3080 pada *Server* dimana *nginx* mendengarkan setiap TCP request yang masuk dan meneruskan ke IP *OpenVPN Client* di *port* 8080 pada perangkat *android* melalui *OpenVPN Server*, sehingga *i-Jetty* pada perangkat *android* dapat di akses secara *remote* menggunakan koneksi 3G maupun koneksi 2G. Pada Gambar 1 terlihat bagaimana perangkat *android* yang memiliki *Dynamic IP Address* dan IP VPN 10.8.0.6 terhubung ke *server* VPN dengan IP VPN 10.8.0.1, sehingga perangkat *android* dapat di akses melalui *OpenVPN Server* yang memiliki IP *Public* 110.139.230.83 dari ISP Telkom. Perangkat Lunak yang dipergunakan:

a. *Ubuntu Linux 12.04.1 LTS 32bit*
b. *OpenVPN Server 2.2.2*
c. *Nginx 1.3.3*
d. *MikroTik RouterOS™*
e. *SuperUser v3.1.3(46) with SU Binary v3.1.1(17)*
f. *Android Kernel 2.6.35.7-perf-CL882825 dragonn@arch #188*
g. *i-jetty 3.1*
h. *OpenVPN Installer for Android 0.2.4*
i. *OpenVPN Settings for Android 0.4.12*
j. *MikroTik WinBox Loader v2.2.18*
k. *PuTTY 0.61*
l. *DropBear SSH Server*
m. *Terminal Emulator*

Perangkat Keras Yang dipergunakan:

a. *Motherboard Advance G41*
b. *Processor Intel Celeron 3.06 GHz,*
c. *Ram 1 GB DDR 2 PC 5400,*
d. *Power Supply Max Power 450Watt,*
e. *Hardisk Samsung 40 GB,*
f. *VGA Nvdia GForce 7200 GS,*
g. *Monitor Samsung SyncMaster 740N,*
h. *Casing SimX,*
i. *Keyboard Mouse SPC,*
j. *MikrotikOS Router*

2. Perlengkapan Pendukung Yang dibutuhkan

Untuk mendukung pada saat pelaksanaan pengujian, diperlukan hardware dan software sebagai berikut:

a. Perangkat Keras yaitu:
   1) Laptop sony Vaio VGNC190 yang digunakan sebagai VPN server, yaitu gerbang antara server VPN dengan klien.
   2) Ponsel mito android T500 yang digunakan sebagai klien VPN.
   3) Jalur data 2 buah, yaitu fixed line pada sisi server dan wireless pada sisi klien. Sis server menggunakan produk ADSL telkomspeedy dan sisi server menggunakan 3G operator telkomsel.
b. Perangkat lunak yaitu:
   1) Windows XP, ini digunakan karena didalamnya sudah terdapat protokol PPTP didalamnya dan pengkonvigurasiannya yang mudah digunakan sebagai VPN server.
   2) Wireshark merupakan perangkat lunak yang digunakan untuk melakukan analisa jaringan komputer dan menganalisa beberapa parameter QoS.

3. Instalasi dan Konfigurasi

Pada sisi server dilakukan instalasi windows XP professional. Sedangkan untuk pengukuran data pengujian, maka perangkat lunak wireshark dan Trafmeter diinstal. Sedangkan pada sisi client diinstal perangkat lunak SymNC. Sedangkan untuk koneksi internet, dibutuhkan pada sisi client maupun pada sisi server. Koneksi yang digunakan untuk sisi klien adalah bersifat *wireless* dan menggunakan 3G. Sedangkan pada sisi server menggunakan *Fixed Line* dari ISP sehingga membutuhkan instalasi seperti modem ADSL dan kabel RJ-45 untuk menyambungkan koneksi internet dari ISP ke laptop yang pada pengujian ini berfungsi sebagai sever.

Sedangkan untuk konfigurasi yaitu, konfigurasi yang dilakukan pada sisi server dengan menggunakan sistem operasi windows XP dengan langkah konfigurasinya yaitu:

a. Klik Start -- control panel --- Network connection.
b. Klik create a new connection --- Next ---- Pilih Setup Advanced Connection ---- Next.

c. Pilih Accept Incomming Connection --- Next----Next Pilih Allow Virtual Private Connections ---- Next.
d. Buat user baru untuk autentikasi VPN dengan memilih add lalu isi user name dan password yang diinginkan .
e. Pada jendela berikutnya Pilih Internet Protocol klik Properties, pada jendela ini adalah untuk memberikan IP kepada client agar bisa berkomunikasi dengan server. Klik OK --- Next Lalu klik Finish. Dan konfigurasi sisi server sudah selesai.

Dilakukan konfigurasi pada modem ADSL agarbisa dilewatkan data *mobile* VPN. Langkah-langkahnya adalah sebagai berikut:

a. Buka *browser* Mozilla,lalu ketikkan alamat IP yang merupakan IP DNS dari modem.
b. Masukkan *username* dan *password*.
c. Pilih Advanced, Virtual Server, VPN Tambahkan Rules PPTP.
d. Pilih Apply lalu *restart* Modem.

Untuk Sisi Klien dilakukan konfigurasi sebagai berikut. Konfigurasi yang dilakukan adalah pernagkat lunak SymNC:

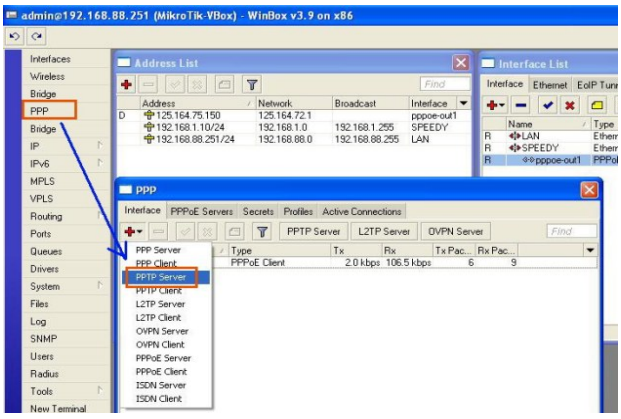
a. Klik icon SymNC pada Ponsel --- Settings.
b. Membuat *account* yang digunakan sebagai autrentikasi sebagai user yang diijinkan untuk berkomunikasi dengan server VPN. Oleh karena itu, account yang akan dibuat harus sama dengan accounts yangdibuat saat pengkonfigurasian server VPN.
c. Setelah selesai membuat account, berikutnya adalah membuat access point, yaitu dengan memilih icon PPTP VPN. Access point ini dibuat sebagai jalur data VPN.

Untuk langkah berikutnya adalah dengan mengkonfigurasi NAS. Nas dikonfigurasi agar server bisa mengakses folder yang di share dan terdapat pada ponsel.

IV. HASIL PENELITIAN DAN PEMBAHASAN

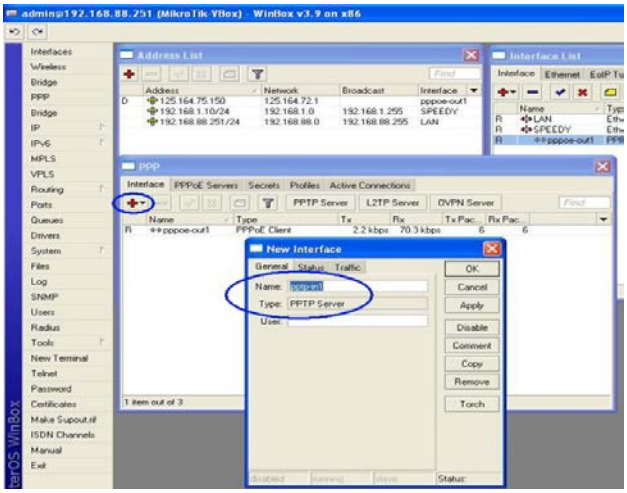
Dilakukan setting VPN pada jaringan 3G sebagai berikut:

1. Langkah pertama adalah melakukan konfigurasi PPP > PPTP server dengan terlebih dahulu mengetahui IP publik internet kita seperti contoh di bawah ini ip publik 125.164.75.150



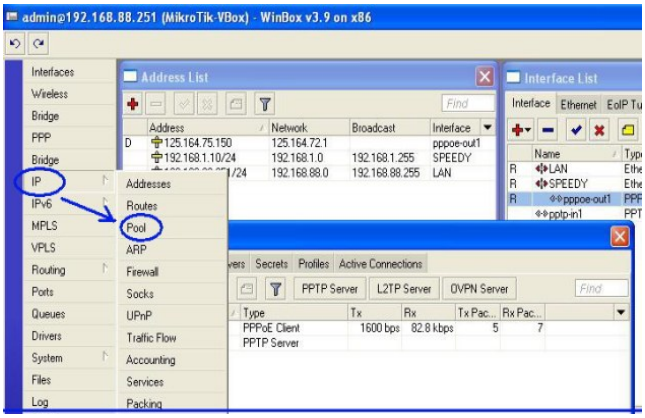
Gambar 7. Konfigurasi server

2. Langkah kedua membuat new interface PPTP server seperti gambar berikut:



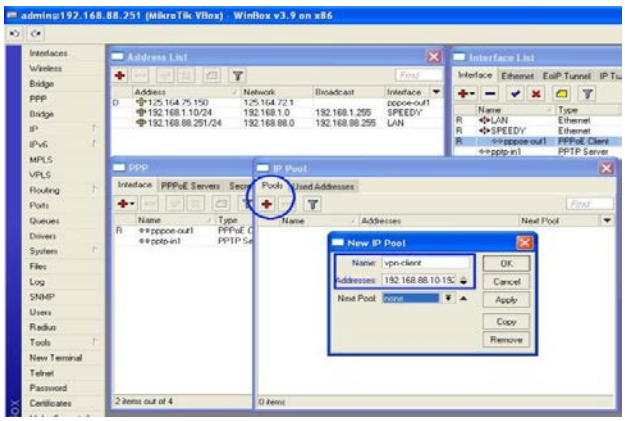
Gambar 8. New Interface PPTPserver

Selanjutnya adalah membuat IP Pool, atau sekelompok IP Address yang akan kita buat untuk mengalokasikan sejumlah IP Address untuk VPN Client per-user yang nanti akan terkoneksi ke Mikrotik VPN Server kita. Selain mengunakan IP Pool, kita juga bisa memberikan IP Address per-user satu per satu. Tapi jika jumlah VPN Client-nya banyak maka cara inilah yang tepat untuk kita lakukan. Caranya : Klik menu IP –> POOL.



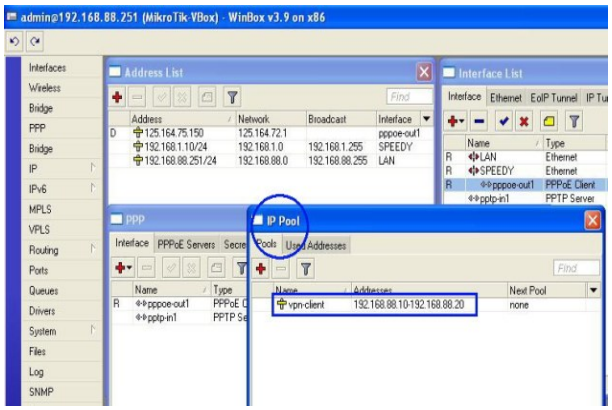
Gambar 9. IP Pool

Dari menu IP -> Pool, selanjutnya buat New IP Pool. Misalnya kita alokasikan IP Address : 192.168.88.10 – 192.168.88.20 dan kita berikan nama vpn-client.



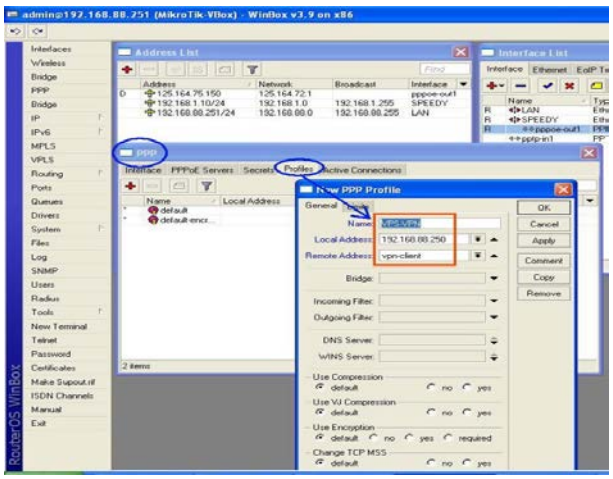
Gambar 10. VPN-Client

Selanjutnya melihat IP Pool yang kita buat telah berhasil dengan baik.



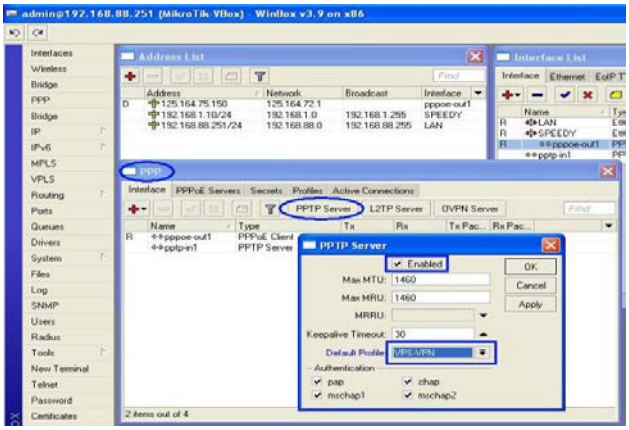
Gambar 11. Hasil pembuatan IPPool

Selanjutnya kita buat sebuah *Profile* dengan nama VPNku. Local Address adalah IP Address yang digunakan sebagai VPN *Gateway* oleh Mikrotik. *Remote Address* adalah IP *Address* yang akan diberikan kepada masing-masing VPN klien dan IP *Address* inilah yang dikenali dan berkomunikasi dengan PC yang lain.



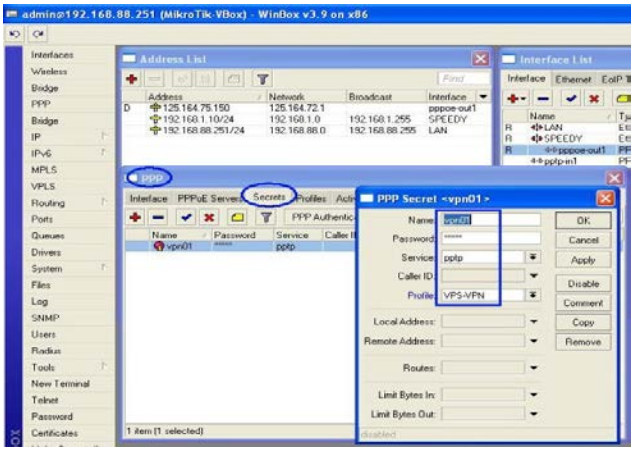
Gambar 12. Profile VPN

Selanjutnya kita klik PPTP SERVER. Option inilah yang menentukan Fitur PPTP SERVER berfungsi apa tidak pada Mikrotik kita. Aktifkan / centang tanda checkmark "ENABLE" lalu pilih Default Profile yang telah kita buat pada langkah keenam.



Gambar 13. Hasil Pembuatan PPTP Server

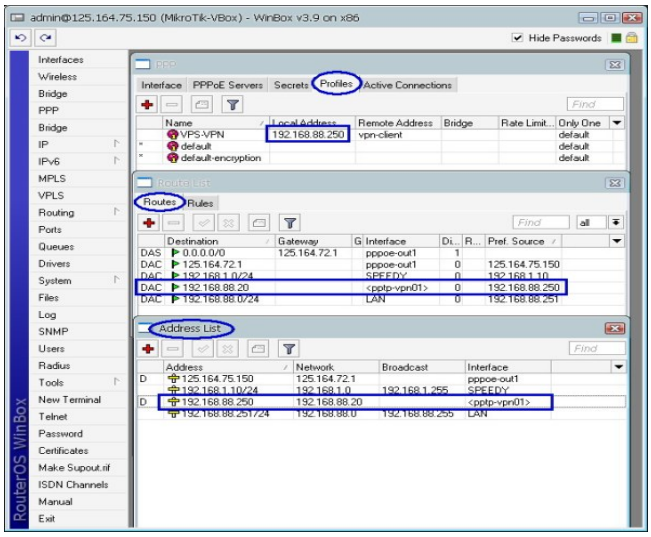
Langkah selanjutnya adalah membuat *User* VPN di menu tab "SECREET". Setting *Username*, *Password*, *Service* : PPTP dan Profile VPS-VPN seperti gambar dibawah ini :



Gambar 14.Pembuatan account pada VPN

Sampai disini tugas membangun VPN Server telah selesai dibuat dan langkah selanjutnya adalah membuat setting VPN *Client* di PC atau Laptop kita.

Kita telah terkoneksi dengan VPN Server dan selanjutnya bisa cek Ping ke IP Client lain yang ada dalam jaringan 1 *Network* dengan Mikrotik (PC *Client* di jaringan kantor), termasuk untuk mengakses semua *resource* yang ada di jaringan LAN tersebut.



Gambar 15. Koneksi dengan VPN untuk Proses Monitoring

Setelah itu dilakukan analisa perbandingan terhadap hasil pengujian dari mobile VPN yaitu jaringan 3G menggunakan protokol PPTP dan ketika hanya menggunakan jaringan 3G saja. Parameter yang dibahas dari performansi adalah sisi troughput dan waktu transfer yang dibutuhkan untuk mengirimkan suatu paket dari klien ke server maupun sebaliknya dari server ke klien.

Throughput merupakan banyaknya bit yang diterima pada suatu node persatuan waktu sedangkan waktu transfer adalah aktu yang dibutuhkan untuk mengirimkan suatu data dari satu node ke node yang lain.

Analisis Pengukuran data dari Klien Ke Server

Pengambilan data untuk pengukuran dilakukan saat klien berupa RTU yang terhubung dengan pompa melakukan hubungan dengan server VPN, yaitu berupa laptop ,dimana pengukuran dilakukan dengan mengirimkan hasil pembacaan pompa pada saat mengidupkan dan mematikan melalui jaringan. Pada pengukuran ini, data yang diamati pada wireshark yaitu data PPP, pada pengujian mobile VPN dan data TCP pada pengujian jaringan 3G sebagai berikut:

TABEL 1. DATA TROUGHPUT DARI KLIEN KE SERVER

No	Data Pengujian	Troughput (Mbit/sec)	
		Mobile VPN Sbg RTU	Jaringan 3G
1	Pengujian 1	0.075	0.229
2	Pengujian 2	0.095	0.235
3	Pengujian 3	0.083	0.201
4	Pengujian 4	0.081	0.200
5	Pengujian 5	0.163	0.196
6	Rata-rata Pengujian	0.099	0.212

TABEL 2. DATA WAKTU TRANSFER DARI KLIEN KE SERVER

No	Data Pengujian	Waktu Transfer (Second)	
		Mobile VPN Sbg RTU	Jaringan 3G
1	Pengujian 1	180	39
2	Pengujian 2	121	44
3	Pengujian 3	65	41
4	Pengujian 4	156	35
5	Pengujian 5	71	40
6	Rata-rata Pengujian	118.6	39.8

Dari hasil pengukuran, maka dapat kita lihat bahwa troughput yang dihasilkan dengan menggunakan VPN yang merupakan RTU terlihat lebih lambat jika dibandingkan dengan troughput menggunakan jaringan. Rata-rata troughput yang didapatkan dari 5 kali pengujian ketika menggunakan mobile VPN yaitu 0.099 Mbit/Sec, sedangkan troughput rata-rata dari jaringan 3G yaitu 0.212 Mbit/sec. Berarti troughput jaringan 3G lebih cepat 141,4 % dibandingkan dengan mobile VPN ketika mentransfer data dari server ke klien.

Sedangkan untuk hasil pengukuran dari waktu transfernya pada 5 kali pengujian di dapat rata-rata mobile VPN yaitu 118, 6, jauh lebih lambatjika dibandingkan dengan waktu transfer dari jaringn 3G, yaitu 39.8 detik. Ini berarti waktu transfer jaringan 3G lebih cepat 170% bila dibandingkan dengan waktu transfer mobile VPN.

Analisis Pengukuran Data Dari Server Ke Klien

Pada pengukuran berikutnya juga mengirimkan hasil pembacaan pompa yang dibuat bentu image dari server ke klien.Pengukuran ini menggunakan wireshark yaitu data PPP pada pengujian mobile VPN / RTU dan data TCP pada pengujian jaringan 3G.

TABEL 3. DATA TROUGHPUT DARI SERVER KE KLIEN

No	Data Pengujian	Troughput (Mbit/sec)	
		Mobile VPN Sbg RTU	Jaringan 3G
1	Pengujian 1	0.184	0.176
2	Pengujian 2	0.195	0.166
3	Pengujian 3	0.199	0.201
4	Pengujian 4	0.223	0.198
5	Pengujian 5	0.201	0.211
6	Rata-rata Pengujian	0.2004	0.190

TABEL 4. DATA WAKTU TRANSFER DARI KLIEN KE SERVER

No	Data Pengujian	Waktu Transfer (Second)	
		Mobile VPN Sbg RTU	Jaringan 3G
1	Pengujian 1	90	91
2	Pengujian 2	96	97
3	Pengujian 3	101	105
4	Pengujian 4	110	109
5	Pengujian 5	95	101
6	Rata-rata Pengujian	98.4	100.6

Hasil yang didapatkan ketika mengirimkan data dari server ke klien, hasilnya berbeda dengan ketika mengirimkan data dari klien ke server. Nilai troughput yang dihasilkan pada saat menggunakan mobile VPN, selalu lebih cepat jika dibandingkan dengan troughput ketika menggunakan jaringan 3G yaitu sebesar 0.190 Mbit/Sec. Hal ini berarti throughput mobile VPN lebih cepat 5.47 % dibandingkan dengan jaringan 3G. Begitu juga untuk waktu transfer, ketika menggunakan mobile VPN lebih cepat bila dibandingkan dengan jaringan 3G. Dari rata-rata yang didapatkan pada 5 kali pengujian untuk mobile VPN yaitu 98.4 detik, sedangkan untuk jaringan 3G yaitu 100.6 detik. Ini berarti waktu transfer mobile VPN 2.23 % lebih cepat bila dibandingkan dengan jaringan 3G.

V. KESIMPULAN

A. Kesimpulan

Dalam paper ini, telah dilakukan perancangan sistem SCADA untuk master stasiun penggerak pompa sekunder pada *water* treatment menggunakan kontroler PLC, melalui interface untuk mengontrol dan memonitor parameter secara real-time melalui layanan 3G VPN.

Sistem yang dirancang menunjukkan bahwa sistem kontrol ini memiliki otomatisasi tingkat tinggi, dan kinerja yang stabil dan dapat diandalkan, terutama dalam hal pengurangan waktu akuisisi dan pemenuhan persyaratan kontrol.

Hasil percobaan komunikasi data dengan menggunakan VPN berhasil dengan baik, walaupun memiliki kecepatan waktu transfer yang berbeda-beda.

DAFTAR PUSTAKA

Aguilera,E.L., Heuse, M., Grunenberger,Y., Rousseau,F., Duda,A., Casademont, J., (2008) An Asymmetric Access Point for Solving the Unfairness Problem in WLAN. IEEE Transaction on Mobile Computing,Vol 7,No.10.

Burgess,M., (2004). Principless of Network And Systems Administration. 2nd Edition. John Wiley and Son.

David Barry, 2002, "VPN Management"., Third Edition 2002, Packet Magazine Cisco

System., USA., 57-60 pp. Feng,C., Anthea ,W.S., Valaee,S., Tan,Z.,(2010).Compressive Sensing Based Positioning Using RSS of WLAN Access Points. IEEE INFOCOM Proceedings.

OMRON, "How Safe is Allowing Remote Access to Omron PLCsVia the Internet and How is it Accomplished".OMRON.2009.

Kompetitif,. (2011). Panduan Penyusunan Dan Seleksi Proposal Kegiatan Kompetitif LIPI Tahun 2012. Lembaga Ilmu Pengetahuan Indonesia - Biro Perencanaan Dan Keuangan. Jakarta.

Kuzminsky,A.M., (2006). EIRPRestrict Downlink Beamforming in WLAN OFDM Systems. IEEE Conference Publication in Signal Processing Advances in Wireless Communications.

Merat,S.,Almuhtadi,W.(2009).Wireless Network Channel Quality Estimation Inside reactor building Using RSSI Measurement of Wireless Sensor Network.IEEE serial no.978-1-4244-3508-1

Pu,C.C,., & Chung, W.Y. (2008), Mitigation of Multipath Fading Effect to Improve Indoor RSSI Performance, *IEEE Sensors Journal Vol 8 no.11.*

Wang,T., Xing,G., Li,M., Jia,W., (2010) Efficient WiFi Deployment Algorithms based on Realistic Mobility Characteristics. IEEE 978-1-4244-7489-9/10.

Yani, A., (2008). Panduan Membangun Jaringan Kmputer (edisi revisi Utility Jaringan). Lokomedia. Yogyakarta.

Yeh,S.C., Hsu,W.H.,Su,M-Y., Chen, C.H.,Liu,K.H. (2009) A Study on Outdoor Positioning Technology Using GPS and WiFi Technology. *Proceedings of the IEEE Conference On Networking, Sensing and Control,Okayama,Japan March 26-29.*

S.Abdallah, A.Adbulkarim, "Methodology to desigy an automated pump plants with PLC control system". Proceedings of the International engineering conference. Mutah-Jordan, 2004, 26-28 April, 373-398.