Jurnal Algoritma, Logika dan Komputasi
Versi Online: *Vol.II (No. 1) : 138 - 150. Th. 2019*
https://journal.ubm.ac.id/index.php/alu *p-ISSN: 2620-620X*
http://dx.doi.org/10.30813/j-alu.v2i1.1574 *e-ISSN: 2621-9840*

PENERAPAN PPTP DAN BCP DENGAN INTER-VLAN PADA TOPOLOGI YANG MENGGUNAKAN 2 ISP SEBAGAI PENGHUBUNG ANTAR DIVISI (Studi Kasus: PT Kenari Djaja Prima)

IMPLEMENTATION OF PPTP AND BCP WITH INTER-VLAN ON THE TOPOLOGY THAT USES 2 ISP AS INTER-DIVISION CONNECTORS (Case Study: PT Kenari Djaja Prima)

Jimmy Gunawan[1)] Halim Agung, hagung@bundamulia.ac.id [(2)]
[1) 2)] Teknik Informatika, Fakultas Teknologi dan Desain, Universitas Bunda Mulia

ABSTRACT

PT Kenari Djaja Prima will create a tunnel between branch offices located far from the central office so that these two offices can retrieve data on the server. As well as forming a local network between branch offices and centers. From the problem, the authors conducted a study and proposed using VLANs to divide divisions, and the tunnel method in the form of PPTP as encryption tunnel to connect with branch offices and BCP methods to forward ethernet packets so that the IP segmentation of headquarters with branches could be connected. From the results of this study, the average maximum Mbps obtained from downloads is 25.87 Mb, the average is at least 1.19 Mb, the average speed is 15.24 Mb, the average time is one minute and thirty seven seconds, and the average delay is 200.28 MS. The conclusion obtained in this study is that division of divisions with VLANs can be overcome, and between divisions have their own VLAN IDs, and can communicate with each other using Inter-VLAN. And use tunnels to connect branch offices with headquarters using PPTP. PPTP as tunnel encryption, EoIP as an ethernet connector and as a VLAN distribution between headquarters and branches. So that the data will be safe until the destination.
***Keywords**: PPTP, QoS, VLAN, Inter-VLAN*

ABSTRAK

PT Kenari Djaja Prima akan membuat *tunnel* antara kantor cabang yang berlokasi jauh dengan kantor pusat sehingga kedua kantor ini bisa mengambil data di *server*. Serta terbentuk jaringan lokal antara kantor cabang dan pusat. Dari masalah yang ada, penulis melakukan penelitian dan mengusulkan menggunakan VLAN untuk membagi divisi, dan metode *tunnel* berupa PPTP sebagai enkripsi *tunnel* untuk terhubung dengan kantor cabang dan metode BCP untuk meneruskan paket *ethernet* sehingga segmentasi IP kantor pusat dengan cabang bisa terhubung. Dari hasil penelitian ini, rata-rata maksimal mbps yang didapat dari *download* 25.87 Mb, rata-rata minimal 1.19 Mb, rata-rata kecepatan 15.24 Mb, rata-rata waktu nya satu menit lewat tiga puluh tujuh detik, dan rata-rata delay 200.28 MS. Kesimpulan yang didapat pada penelitian ini adalah pembagian divisi dengan VLAN sudah bisa diatasi, dan antar divisi memiliki VLAN ID masing-masing, dan bisa saling komunikasi menggunakan *Inter*-VLAN. Dan menggunakan *tunnel* untuk menghubungkan kantor cabang dengan kantor pusat menggunakan PPTP. PPTP sebagai enkripsi *tunnel*, EoIP sebagai penghubung *ethernet* dan sebagai distribusi VLAN antar kantor pusat dan cabang. Sehingga data akan aman sampai dengan tujuan.
Kata Kunci: PPTP, QoS, VLAN, *Inter*-VLAN

Jurnal Algoritma, Logika dan Komputasi
Vol.II (No. 1) : 138 - 150. Th. 2019
p-ISSN: 2620-620X
e-ISSN: 2621-9840

PENDAHULUAN

Kebutuhan akan komunikasi menjadikan teknologi informasi sebagai salah satu aspek penting dalam proses bisnis. Perkembangan teknologi komunikasi dan teknologi komputer yang berkembang saat ini, dimana setiap aspek kehidupan telah menggunakan jasa-jasanya mulai dari perkantoran, pendidikan, rumah tangga, hingga pekerjaan professional yang menggunakan teknologinya. Sampai dengan saat ini, jaringan komputer atau *intranet private* masih banyak yang menggunakan *leased line* dengan estimasi biaya yang cukup mahal. Sebagian perusahaan yang mempunyai anak perusahaan atau cabang menggunakan *leased line* agar kedua peruasahaan dapat saling terhubung dan bertukar data, karena lebih aman dengan alasan jaringan seperti ini secara fisik terpisah dengan jaringan publik. Namun jaringan seperti ini akan menimbulkan biaya yang cukup besar seiring dengan jarak dan besarnya wilayah jaringan tersebut.

Internet merupakan jaringan publik yang telah tersebar luas dan mendunia sehingga dapat digunakan dengan mudah. Dengan adanya *internet* maka dapat dimanfaatkan untuk membangun jaringan *Virtual Private Network* (VPN). VPN mengurangi biaya karena menghindari penggunaan *leased line* tertentu yang secara tersendiri menghubungkan *remote office* ke sebuah *intranet private*. VPN adalah teknik pengaman jaringan yang berkerja dengan cara membuat suatu *tunnel* antara satu tempat ke tempat lain yang dalam hal ini yaitu kantor pusat dengan kantor cabang yang jaraknya saling berjauhan.

Dalam studi kasus yang terdapat dalam skripsi, menggunakan kasus yang terdapat dalam PT Kenari Djaja Prima, dimana setiap kantor pusat dan cabang memiliki beberapa departemen yang berbeda. Setiap departemen nantinya akan dipisah menjadi beberapa *segment* seperti departemen direksi kantor pusat dengan departemen direksi kantor cabang yang saling terhubung dengan satu *segment*.

Metode *tunneling*, *Point to Point tunneling Protocol (*PPTP) akan digunakan untuk menghubungkan kantor pusat dengan kantor cabang yang diteruskan dalam bentuk paket *ethernet*, paket *ethernet* yang akan dikirimkan dapat diteruskan oleh metode *Bridge Control Protocol* (BCP) ke jaringan lokal. sedangkan untuk memisahkan departemen antar kantor pusat dengan departemen kantor cabang dapat menggunakan jaringan *Virtual Local Area Network* (VLAN) yang nantinya setiap departemen akan diberikan sebuah Identitas(ID) sesuai dengan departemen pada kantor pusat dan cabang.

METODE PENELITIAN

Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagi sumber daya, berkomunikasi dan dapat mengakses informasi. Tujuan jaringan komputer agar jaringan komputer dapat meminta dan memberikan layanan. Pihak yang meminta atau menerima layanan disebut *client* sedangkan yang memberikan atau mengirim layanan disebut *server*. Desain ini disebut dengan *system client-server*. Media transmisi merupakan jalur yang digunakan untuk dapat melakukan perpindahan data, baik berupa kabel maupun tanpa kabel. [1]

Topologi

Topologi jaringan dalam telekomunikasi adalah suatu cara menghubungkan perangkat telekomunikasi yang satu dengan yang lainnya sehingga membentuk jaringan. Jaringan tersebut akan saling berhubungan satu sama lain membentuk sebah komunikasi data. [2]

Virtual Private Network (VPN)

VPN adalah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dengan jaringan lokal. VPN adalah proses dimana jaringan umum *public network* atau *internet* diamankan kemudian difungsikan menjadi sebuah jaringan *private network*. [3]

Jurnal Algoritma, Logika dan Komputasi
Vol.II (No. 1) : 138 - 150. Th. 2019
p-ISSN: 2620-620X
e-ISSN: 2621-9840

Bridge Control Protocol (BCP)

Bridge Control Protocol (BCP) adalah sebuah protokol yang memungkinkan untuk meneruskan paket *ethernet* melalui link PPP atau metode *tunneling* VPN seperti PPTP, L2TP, dan EoIP.

BCP merupakan bagian independen dari *tunneling* PPP, tidak terkait dengan alamat IP dari antarmuka PPP, *bridging*, dan *routing* dapat terjadi pada saat yang sama secara independen. BCP dapat digunakan *tunnel* VPN atau *link* WDS melalui jaringan nirkabel dan seolah-olah terhubung namun tidak ada kabel secara fisik yang tersambung. Contoh implementasi BCP adalah ketika kita ingin menghubungkan 2 *site* agar bisa menggunakan *segment* IP yang sama, tetapi pada saat yang sama juga dibutuhkan enkripsi untuk menjaga data yang dipertukarkan. [4]

Virtual Local Area Network (VLAN)

VLAN merupakan sebuah teknologi yang digunakan untuk memecah wilayah *broadcast* dalam sebuah perangkat *switch.* Pada dasarnya semua *port switch* akan digabungkan dalam satu wilayah *broadcast* yang sama. Jadi, apabila ada salah satu komputer yang mengirimkan data secara *broadcast*, maka data tersebut akan diteruskan ke semua *port* selain *port* yang digunakan oleh komputer pengirim untuk mengirimkan data *broadcast* tadi.

Quality of Service (QoS)

Terminologi yang digunakan untuk mendefinisikan karakteristik layanan (*service*) jaringan guna mengetahui seberapa baik kualitas layanan tersebut. [5]

Berdasarkan penelitian yang dilakukan [1] *Quality of Service* ada beberapa parameter yaitu *throughput*, *bandwidth* dan *delay*.

Server Message Block (SMB)

SMB adalah *protocol client/server* yang ditujukan sebagai layanan untuk berbagi berkas (*file sharing)* di dalam sebuah jaringan. Protokol ini sering digunakan dalam sistem operasi *windows* dan IBM. SMB awalnya menggunakan protokol NetBios sebagai protokol dimana ia berjalan, sebelum menggunakan protokol NetBios *over* TCP/IP (NBT) sebagai protokol lapisan *transport*-nya. Dengan begitu, SMB juga dapat digunakan dalam sebuah jaringan TCP/IP yang lebih luas dukungannya.

Bit Rate

Bit Rate adalah jumlah rata- rata nilai *bit* yang diperlukan untuk mengirimkan data dalam satuan waktu tertentu. Pengukuran umum dari *bit rate* biasanya menggunakan istilah *kilobitpersecond* (Kbps) dan *Megabitpersecond* (Mbps). Apapun unit yang tengah diukur, semakin tinggi angka *bitrate*, maka kualitas *file* semakin bagus atau semakin cepat. Bit Rate yang didapat saat pengiriman paket dari *server* ke *client*. Satu MB sama dengan 1.024 *kiloByte* dan itu artinya 1 MB sama dengan 1.048.576 *Byte*, bukan sejuta *Byte*. MBps adalah singkatan dari *Mega Byte Per Second* adalah satuan untuk mengukur kecepatan *internet* per detik dengan menggunakan satuan *Byte*.

Analisis Kebutuhan Fungsional

1. Metode *tunneling* digunakan untuk membuat terowongan pada jalur publik agar mempunyai jalur tersendiri yang memiliki enkripsi sehingga tidak terlihat oleh oknum-oknum tidak bertanggung jawab yang terhubung ke kantor pusat.
2. Metode BCP digunakan untuk membuat segmentasi yang sama antar VLAN kantor cabang dengan VLAN kantor pusat, sehingga segmentasi kantor cabang terhubung dengan VLAN kantor pusat meskipun berada pada lokasi yang berbeda.
3. Kantor cabang dapat mengolah data pada *server* kantor pusat menggunakan *Microsoft Great Plains*.

Analisis Kebutuhan Non-Fungsional

1. Perangkat Keras (*Hardware*)

Jurnal Algoritma, Logika dan Komputasi
Vol.II (No. 1) : 138 - 150. Th. 2019
p-ISSN: 2620-620X
e-ISSN: 2621-9840

Tabel 1. Spesifikasi *Router*

Router	**Mikrotik RB1100AHX2**	**Mikrotik RB962UiGS**
Digunakan	Kantor Pusat	Kantor Cabang
CPU	P2020 1066MHz Dual Core	QCA9558 720MHz
Main Storage	64MB	16MB
RAM	1.5GB	128MB
LAN Port	13	5
Giga Bit	Yes	Yes
License	Level 6	Level 4

Tabel 2. Spesifikasi *Switch*

Router	**Digunakan**	**LAN Port**	***Giga Bit***
Cisco 2960 Catalyst	Kantor Pusat	24	Yes
Mikrotik RB95Ui-5ac2nD (hAP-AC-Lite)	Kantor Cabang	5	No

2. Perangkat Lunak (*Software*)

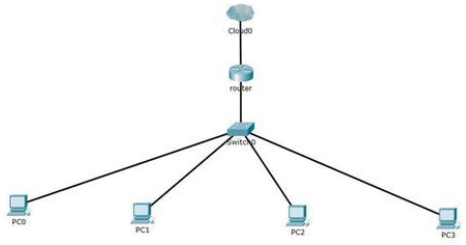
Tabel 3. Aplikasi Digunakan

Nama *Software*	**Versi**
Bandwidth meter pro	2.6
Wireshark	2.2.5
Winbox	3.11

PT Kenari Djaja Prima

PT Kenari Djaja Prima sekarang berpusat di Sunter, dan ada banyak cabang di seluruh Indonesia. Namun setiap cabang hanya cabang toko, dan hanya mengambil data di *server*. Namun ada rencana untuk membuat toko cabang menjadi kantor yang ada beberapa divisi mengirim dan mengambil data penting di *server*. Kantor cabang PT Kenari Djaja Prima menggunakan ISP lain untuk terhubung ke kantor pusat. Maka dari itu perlu membuat *tunneling* yang terenkripsi, dan karena ada beberapa divisi, maka dibuatkan juga VLAN untuk mendistri*Bus*ikan atau membedakan antar divisi pada saat melakukan penukaran *data*. *Bandwidth* yang digunakan adalah yang *bandwidth* terkecil pada kedua sisi kantor.

Rancangan Topologi di PT Kenari Djaja Prima



Gambar 1. Topologi

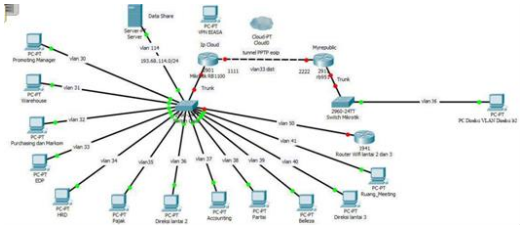
Pada saat melakukan *sharing centre*, karena semua terdeteksi satu segmen, maka akan terlihat semua *device* sehingga bisa saja terjadi pertukaran data jikalau orang salah memilih PC yang mau dikirim atau antar divisi bisa saja saling menukar data yang beresiko membahayakan kebocoran data. Dengan terlihatnya semua *device*, bisa saja terjadi pertukaran data dimana mungkin ada karyawan yang salah memilih nama komputer nya atau antar divisi bisa saling menukar *data* yang mungkin bisa beresiko untuk kantor karena ada kebocoran *data*.

Rancangan Topologi yang Diusulkan

Tabel 4. *Bandwidth* dan IP *Internet*

Keterangan	**Kantor Pusat**	**Kantor Cabang**
IP *Internet*	573204f365e4.sn.mynetname.net	158.140.177.106
Upload	30 Mbps	50 Mbps
Download	30 Mbps	50 Mbps
DNS	202.147.192.29 192.168.1.1	192.168.100.1

Jurnal Algoritma, Logika dan Komputasi
Vol.II (No. 1) : 138 - 150. Th. 2019
p-ISSN: 2620-620X
e-ISSN: 2621-9840



Gambar 2. Topologi *Tunneling* Usulan

Pengimplementasian pada topologi yang digunakan di gambar 2 menggunakan jaringan *internet*. Dikarenakan lokasi kantor cabang yang terletak cukup jauh dengan kantor pusat, maka kantor cabang menggunakan ISP lain. Maka dari itu dilakukan *port-forwading* dari *router* ISP ke *router* mikrotik sehingga bisa melakukan *tunnel*. Walaupun disana terlihat berbeda *bandwidth* yang cukup besar, tetapi jika ingin melakukan pertukaran *data*, maka *bandwidth* terkecil lah yang akan digunakan oleh kedua sisi pusat dan cabang. Karena *bandwidth* yang disediakan dikantor pusat hanya 30 Mbit, maka data yang masuk ke cabang pun hanya 30 Mbit walaupun dia memiliki *bandwidth* yang lebih besar dibandingkan pusat.

Topologi yang diusulkan adalah menggunakan topologi *tree*. Karena pada topologi *tree* memiliki *level* teratas sebagai *root* yang menjadi pusat utama komunikasi bagi seluruh komputer lain saling terkoneksi dengannya yaitu *router* Mikrotik yang disesuaikan dengan kasus pada kantor PT Kenari Djaja Prima.

Kantor PT Kenari Djaja Prima memiliki jaringan skala besar, dan terdapat banyak divisi, sehingga diperlukan pengelompokan divisi agar mudah untuk di kendalikan. Adanya *hub* pusat sebagai pusat data jaringan dan kendali jaringan. Semua komunikasi akan melewati *hub* dan adanya kabel *backbone*.

Topologi yang diajukan adalah dua ISP yang berbeda tetapi akan di *tunnel* menggunakan PPTP, dan disisipi VLAN melalui PPTP, sehingga pada saat melakukan penukaran atau pengiriman *data*, antar divisi tidak akan saling tertukar, dan begitu juga dengan di posisi kantor cabang. Divisi-divisi yang ada di kantor cabang dan pusat, akan terhubung melalui VLAN yang di salurkan melalui PPTP *tunnel*, kemudian ada VLAN distribusi yang akan didistribusikan ke PC melalui LAN.

Tabel 5. *Tunnel* ID

Keterangan	**ID *Password***
PPTP *Secret*	cobacoba

Tabel 6. VLAN ID

VLAN	**Keterangan**
30	*Promoting Manager*
31	*Warehouse*
32	*Purchasing Marcom*
33	EDP
34	HRD
35	*Tax*
36	Direksi Lt2
37	*Accounting*
38	Partisi
39	Belleza
40	Direksi Lt3
41	Ruang_Meeting
50	*Wifi User*
114	*Data Server*

Pemilihan Metode

Dalam penelitian ini metode yang digunakan adalah metode *tunneling*. Salah satu model metode *tunneling* adalah PPTP. PPTP merupakan salah satu VPN yang paling mudah untuk disiapkan. PPTP juga mendukung hampir semua sistem operasi. Komunikasi dalam PPTP menggunakan *protocol* TCP *port* 1723 dan menggunakan IP *protocol* 47 (GRE) untuk enkapsulasi paket datanya.

Setelah melalui tahap metode PPTP, data yang telah dienkripsi akan dikirim melalui *bridge* menggunakan BCP (*Bridge Control Protocol)* sehingga segmentasi IP pada kantor pusat dan kantor cabang memiliki segmentasi IP yang sama. BCP harus di konfigurasikan di kedua sisi *router*.

Model PPDIOO

Dalam penulisan ini metode pengembangan sistem yang digunakan adalah model PPDIOO. Adapun alasan penulis menggunakan model ini karena

Jurnal Algoritma, Logika dan Komputasi
Vol.II (No. 1) : 138 - 150. Th. 2019
p-ISSN: 2620-620X
e-ISSN: 2621-9840

lebih meningkatkan kecepatan akses ke aplikasi-aplikasi (*software*) dan layanan (*services*) yang ada di kantor pusat, dengan meningkatkan keandalan, ketersediaan, keamanan, skalabilitas dan kinerja.

PPDIOO mendeskripsikan sebuah model siklus hidup jaringan dengan konsep jaringan yaitu:

1. Fase *Prepare* (Persiapan)
   Menetapkan kebutuhan organisasi dan bisnis, seperti *router, switch managed* dan *switch unmanaged* serta kabel LAN untuk membangun jaringan pada kantor pusat serta membangun *tunnel* untuk menghubungkan kantor cabang.
2. Fase *Plan* (Perencanaan)
   Fase ini membutuhkan waktu sebanyak 4 bulan yang terbagi dalam analisis kebutuhan, pemilihan metode, perancangan topologi, implementasi, pengujian, pemeliharaan dan perbaikan. Kebutuhan pada topologi jaringan ini membutuhkan sekitar 25 Mbps.
3. Fase *Design* (Desain)
   Desain topologi jaringan yang akan dibentuk adalah topologi *tree* karena kantor pusat memiliki *level* teratas sebagai *root* yang menjadi pusat utama komunikasi bagi seluruh komputer lain saling terkoneksi dengannya yaitu *router* Mikrotik yang disesuaikan dengan kasus pada kantor PT Kenari Djaja Prima.
4. Fase *Implement* (Implementasi)
   Pada fase ini, peralatan-peralatan baru dilakukan instalasi dan di konfigurasi, sesuai spesifikasi desain. Konfigurasi yang dilakukan pertama adalah pada kantor pusat pada *router* utama yaitu membuat IP Add, VLAN, serta PPTP *server* yang terdiri dari *username* dan *password* dan *bridge* untuk BCP yang akan menghubungkan VLAN pada kantor cabang melalui PPTP.
5. Fase *Operate* (Operasional)
   Mencoba melakukan pengujian terhadap kinerja jaringan pada saat transmisi data dari kantor cabang ke kantor pusat. Pengujiannya terdiri dari beberapa parameter dari QOS yang meliputi *bandwidth, throughput, delay.*
6. Fase *Optimize* (Optimalisasi)
   Memeriksa kinerja jaringan sesuai dengan harapan perusahaan dan me *monitoring* jaringan agar terhindar dari masalah yang mungkin terjadi atau membahayakan keamanan data perusahaan.

Proses VPN *tunnel* PPTP

Proses VPN *tunnel* PPTP dimulai dari jika ada sebuah PC dari VLAN 36 yang ada di kantor cabang, mengambil data dari *server* yang berada di kantor pusat VLAN 114. Kemudian *router gateway* kantor pusat akan memeriksa otentifikasi *username* dan *password* dari *router* kantor cabang. Proses otentifikasi menggunakan protokol CHAP yang direkomendasikan sebagai metode *authentication* PPP *protocol*, yang memberikan suatu *authentication* terenkripsi dua arah yang mana lebih *secure* daripada PAP. Jika jalur sudah tersambung, kedua *server* di masing-masing ujung saling mengirim pesan. Setelah pesan terkirim, sisi *remote* yang diujung akan merespon dengan fungsi '*hash'* satu arah menggunakan *Message Digest* 5 (MD5) dengan memanfaatkan *user* dan *password router* pada kantor pusat. Kedua sisi ujung *router* harus mempunyai konfigurasi yang sama dalam PPP *protocol*.

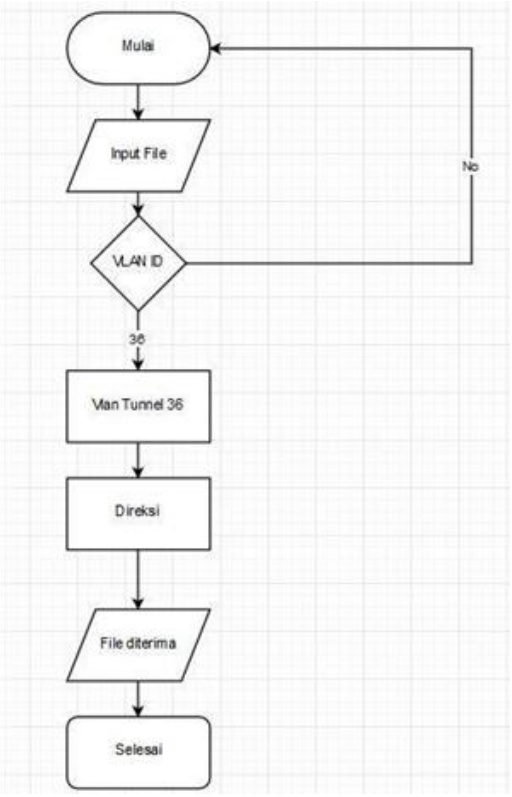
Setelah pemeriksaaan otentifikasi, maka data akan siap dikirim ke kantor cabang, data yang dikirim akan melalui proses enkripsi. Proses enkripsi akan dilakukan oleh metode *tunnel* PPTP menggunakan algoritma 3DES, algoritma *Triple* DES digunakan untuk mengenkripsi paket yang melalui sebuah *point to point link*. *Triple*-DES berarti bahwa algoritma DES diterapkan tiga kali pada data yang akan dienkripsi sebelum dikirim melewati saluran komunikasi. Varian yang digunakan adalah DES-EDE3-KBK. Algoritma DES-EDE3-KBK adalah varian sederhana dari DES-CBC algoritma. Dalam EDE3-DES-CBC, sebuah Inisialisasi Vektor (IV) adalah XOR'd dengan 64 bit pertama (8 oktet) blok *plaintext* (P1). Fungsi pembangkitan kunci *Des* diiterasi sebanyak 3 kali, enkripsi (E) diikuti oleh dekripsi (D) diikuti oleh enkripsi (E), dan menghasilkan *ciphertext* (C1) untuk blok tersebut. Setiap iterasi

Jurnal Algoritma, Logika dan Komputasi
Vol.II (No. 1) : 138 - 150. Th. 2019
p-ISSN: 2620-620X
e-ISSN: 2621-9840

menggunakan kunci independen: k1, k2, k3. Untuk blok berturut-turut, blok *ciphertext* sebelumnya di XOR dengan 8-*octet* blok *plaintext* (Pi). Fungsi enkripsi DES-EDE3 menghasilkan *ciphertext* (Ci) untuk blok tersebut.

Untuk mendekripsi, urutan fungsi dibalik: mendekripsi dengan k3, mendekripsi dengan k2, mendekripsi dengan k1, dan XOR dengan *ciphertext* sebelumnya blok. Ketika ketiga kunci (k1, k2 k3) adalah sama, DES-EDE3-KBK adalah setara dengan DES-CBC. Kemudian setelah dienkripsi data akan menjadi IP *datagram* yang berisi paket PPP yang terenkripsi dan kemudian dikirim melalui PPTP *tunnel* melewati protokol GRE menuju PPTP *client. Client* PPTP memeriksa IP *datagram* dan mendekripsi paket PPP, dan kemudian mengarahkan paket yang terdekripsi ke jaringan *private* melalui protokol BCP.

Flowchart VLAN



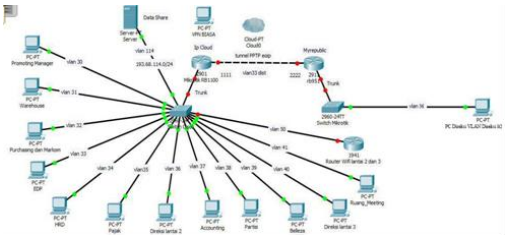
Gambar 3. *Flowchart* VLAN

1. Diawali jika ada yang ingin mengirim *file*, maka sistem akan mengecek VLAN ID.
2. Jika VLAN ID 36 maka akan diarahkan ke VLAN 36 divisi Direksi.
3. Setelah itu *file* diterima oleh divisi yang sesuai dengan VLAN ID.

HASIL DAN PEMBAHASAN

Implementasi Jaringan

Setelah persiapan kebutuhan perangkat lunak dan perangkat keras telah tersedia maka selanjutnya akan dijelaskan bagaimana membangun jaringan *tunneling*.



Gambar 4. Topologi Implementasi

Pada topologi ini, terlihat bahwa kantor memiliki IP *public* dinamis maka menggunakan IP *cloud* yang bisa *update* IP dinamis secara otomatis (WAN) 573204f365e4.sn.mynetname.net. Jika di posisi Kantor IP WAN tersebut sudah statis langsung di *router* Mikrotik tanpa perlu di *port forwading* sehingga bisa langsung di *remote* langsung. Selain itu dalam penelitian ini memiliki 14 VLAN yang mewakili masing - masing divisi yang akan diberikan IP *Local* 193.68.30.0/24 untuk VLAN ID 30, 193.68.31.0/24 untuk VLAN ID 31, dan seterusnya VLAN ID mengikuti segmen ke 3 dari IP *address.* Penulis mengalamatkan IP tersebut dengan *subnet* /24 karena IP yang bisa dipakai adalah 255 IP dan menggunakan DHCP untuk pembagian IP *local* secara dinamis ke setiap PC dan akan di *make static* yang artinya mengunci *Mac – address* dan IP setiap komputer, sehingga tidak akan bisa menggunakan IP sembarangan. Di setiap VLAN ini diharapkan bisa saling berkomunikasi antar VLAN ID yang sama maupun di posisi kantor pusat dengan kantor cabang.

Jurnal Algoritma, Logika dan Komputasi
Vol.II (No. 1) : 138 - 150. Th. 2019
p-ISSN: 2620-620X
e-ISSN: 2621-9840

Konfigurasi dasar yang harus dimiliki oleh kedua *router* baik kantor pusat atau kantor cabang tentunya adalah IP *address*, *default gateway* ke ISP, konfigurasi DNS, maupun konfigurasi NAT dengan *action Masquerade* untuk bisa menjamin komputer pada masing-masing jaringan dapat mengakses *internet* dengan cara menerjemahkan IP *local* menjadi WAN.

Setelah konfigurasi seperti IP *address, gateway, DNS, Firewall NAT Masquerade,* pastikan *router* tersebut dapat mengakses *internet* dengan cara membuka menu *new terminal* di *winbox* dan menggunakan CLI untuk ping ke *google.com.*

Kemudian dilakukan konfigurasi PPTP sehingga bisa terhubung ke kantor cabang. *Router* kantor pusat bertindak sebagai PPTP *server* dengan *router* kantor cabang sebagai PPTP *client.* Untuk membangun koneksi ini diskenariokan bahwa *local address* yang akan digunakan kantor pusat adalah 1.1.1.1 sedangkan kantor cabang 2.2.2.2. IP *address* tersebut hanya akan digunakan untuk saling mengenal antara *router-router* pada saat akan membuat *tunnel*. Yang pertama harus dipersiapkan adalah membuat *interface bridge* sebagai *interface* yang akan ditempatkan *interface* PPTP jika PPTP *client* terkoneksi ke PPTP *server*. Kemudian setelah membuat *interface bridge*, maka langkah selanjutnya adalah memasukan *port Trunk.*

Kemudian membuat VLAN yang akan *tunnel* mengarah ke *interface bridge*, sedangkan VLAN-VLAN yang lain diarahkan ke *ether 10* yang bertindak sebagai *port trunk. Interface ether 10* yang akan dimasukan ke *bridge* karena *interface ether* 10 adalah *port trunk* agar VLAN dapat didistribusikan melalui *tunnel*. Terlihat hanya ada 1 *interface bridge*. Penulis membuat hanya 1 *interface bridge*, karena cukup 1 *bridge* saja, jalur VLAN 36 sudah bisa mengakses semua VLAN, dan fungsi *bridge* agar VLAN bisa ter-enkapsulasi dan *segment* yang lewat diantara VLAN yang lain bisa dibedakan jika ada tambahan VLAN lain. *Interface bridge* ini berperan penghubung antar VLAN *tunneling* dengan VLAN distribusi, sehingga paket dikirim dari VLAN distribusi, peran *bridge* ini menghubungkan paket tersebut ke VLAN *tunneling* dan menuju ke *bridge* kantor cabang.

Kemudian setelah langkah ini membuat PPP *profile* yang akan menjadi *profile* PPTP. PPTP *profile* memiliki parameter *bridge* yang nantinya akan kita isi dengan *interface bridge* yang sudah kita buat tadi untuk *interface* PPTP jika sudah ada koneksi PPTP.

Kemudian membuat PPP *secret* untuk menentukan siapa yang berhak untuk bisa terkoneksi ke PPTP *server*. Pertama yang dilakukan adalah menentukan *Username* yang akan digunakan oleh *router* kantor cabang pada saat akan membuat koneksi dengan *router* kantor pusat. *Username* beserta *password* tersebut harus dikonfigurasikan pada *router* kantor pusat. Untuk konfigurasi *username* dan *password* nya menggunakan PPP *secret* dan mengisi *profile* yang tadi sudah dibuat.

Setelah konfigurasi PPP *secret* maka akan terlihat IP *dynamic* yang didapat oleh *router* kantor, dapat dilihat di gambar IP *address* PPTP berikut ini. Kemudian mengaktifkan PPTP *server*. Jika menggunakan *winbox*, maka konfigurasi dapat dilakukan dengan cara memilih PPTP *server*.

Sampai pada tahapan ini, konfigurasi pada *router* kantor pusat untuk mengaktifkan PPTP *server* sudah selesai. Setelah ini di *router* kantor pusat, di IP *address* akan terlihat IP *Remote Address* dan *Local Addres*s dari *router* kantor cabang jika sudah terkoneksi.

Disini sudah terlihat IP dari PPTP kantor cabang sudah terkoneksi dengan baik dengan kantor pusat, terlihat lambang D yang artinya dinamis. Maka sudah bisa dilihat dari *router* kantor pusat melakukan *ping* terhadap kantor cabang.

Setelah tahap ini, hanya membuat IP DHCP *Server* pada *router* pusat, sehingga nanti nya jika ada komputer yang memasang kabel LAN, akan mendapatkan IP secara dinamis yang VLAN ID nya sesuai dengan divisinya.

Jurnal Algoritma, Logika dan Komputasi
Vol.II (No. 1) : 138 - 150. Th. 2019
p-ISSN: 2620-620X
e-ISSN: 2621-9840

Komputer-komputer ini akan mendapatkan IP, *subnet*, *gateway*, dan DNS secara otomatis. Tentu IP yang didapat sesuai dengan divisi dan VLAN ID nya.

Pembagiannya untuk kantor adalah 193.68.36.101-193.68.36.254 dimana .36 adalah VLAN ID, 61 sampai 254 adalah *range* IP yang bisa dipakai oleh komputer-komputer. Penulis sengaja mengkosongkan .2 sampai .60, untuk antisipasi perangkat yang perlu IP *Statis.*

Konfigurasi Cabang

Sedangkan sisi cabang menggunakan ISP abc yang IP (WAN) nya adalah 158.140.177.106 menggunakan *router* Huawei yang IP *local* (LAN) nya 192.168.100.0/24, tidak bisa menggunakan fitur *tunnel* EoIP atau PPTP dan VLAN, maka dari itu Penulis menggunakan *router* Mikrotik agar bisa membuat *tunnel* dengan kantor dan mendistri*Bus*ikan VLAN. Dikarenakan *router* Mikrotik yang bergerak dibelakang *router* Huawei, maka penulis melakukan *port forwading* dengan tujuan ip *router* Mikrotik yang sudah penulis alamatkan IP Mikrotik adalah 192.168.100.3. Fungsi *port forwading* ini adalah mengoper *request* IP ke dalam jaringan *local* nya sehingga jika kita sedang diluar kota atau diluar kantor, jika ada kendala pada *router*, maka kita membuka *web* dengan protokol TCP HTTP untuk meng- *remote router* tersebut. Dsini penulis akan mengoper *router* HUAWEI menjadi *router* Mikrotik yang dapat diakses diluar atau di *remote*.

Pertama-tama adalah *login* terlebih dahulu kedalam *gateway router* ISP cabang untuk mengatur *port forwading*. Terlihat menu *Forward Rules -> Port mapping configuration* untuk mengatur konfigurasi *port forwading* ke *router* Mikrotik yang IP nya 192.168.100.3 sehingga akan terlihat seperti ini jika kita membuka IP *public* cabang.

Jika di *remote* langsung dari *web* via HTTP dengan memasukan IP Publik kantor cabang, akan langsung muncul halaman Mikrotik. Selanjutnya yang perlu dilakukan *router* kantor cabang adalah membuat *bridge* sama seperti kantor pusat, untuk bisa mengaktifkan fungsi protokol BCP *(Bridge Control Protocol). Interface bridge2* yang akan menjadi *interface bridge* oleh PPTP *client*.

Ether3 bertindak sebagai *port trunk* VLAN di kantor cabang. Setelah itu mengaktifkan PPP *profile* dan mengarahkan parameter *bridge* kepada *interface bridge2* yang dinamakan *PPPBridge*.

Setelah tahap itu, selanjutnya mengaktifkan *interface* PPTP *client* dengan menggunakan *username* dan *password* yang sudah dikonfigurasikan pada *router* kantor sebelumnya. Parameter lain yang harus dikonfigurasikan adalah *connect-to* yang harus diisikan IP *address internet* dari *router* kantor. Parameter ini berguna sebagai petunjuk kemana *router* cabang akan mencari PPTP *server* nya. Dan *profile* diisi dengan *profile PPPBridge* yang sudah dibuat tadi.

Setelah ini di *router* kantor cabang, di IP *address* akan terlihat IP *Remote Address* dan *Local Address* dari *router* kantor pusat.

Maka selanjutnya IP DHCP tidak perlu dibuat di kantor cabang karena komputer-komputer pada kantor cabang akan mendapatkan IP DHCP dari *router* kantor pusat. Komputer-komputer bisa mendapatkan IP secara dinamis yang sesuai dengan VLAN ID nya dan divisinya karena kantor pusat sudah membuat IP DHCP dan di arahkan ke *bridge*, karena *bridge* akan menghubungkan interface VLAN antara kantor pusat dan cabang menggunakan metode BCP (*Bridge Control Protocol)*.

Konfigurasi *Switch* Pusat (Cisco)

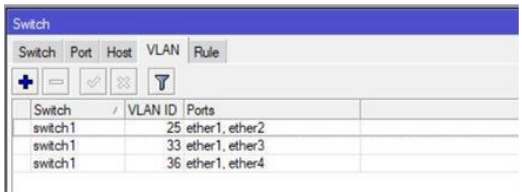
Konfigurasi *switch* Cisco untuk mendistri*Bus*ikan VLAN ke divisi adalah mengatur *port mode trunk*, yaitu *port* 24. Sedangkan *port-port* lainnya adalah *port mode access* yang mendistri*Bus*ikan VLAN ke komputer-komputer. Pertama membuat dulu VLAN-VLAN di *switch.* Kemudian masukan VLAN ke port dengan *mode access*. Sehingga *port-port* VLAN bisa terdistribusi dengan baik ke komputer-komputer.

Jurnal Algoritma, Logika dan Komputasi
Vol.II (No. 1) : 138 - 150. Th. 2019
p-ISSN: 2620-620X
e-ISSN: 2621-9840

Konfigurasi *Switch* Cabang

Dalam tahap ini adalah konfigurasi *switch* untuk mendistri*Bus*ikan VLAN ke divisi. Pertama yang harus diperhatikan adalah *router* yang harus memiliki *Switch-Chip* yang bisa dijadikan menjadi *switch.* Pertama yang dilakukan adalah membuka menu *switch* di menu winbox. Kemudian menjadikan *ether 2, ether 3,* dan *ether 4,* sebagai *slave port* dan *ether 1* sebagai *master port* yang akan dijadikan *trunk port* yang berperan sebagai pengantar VLAN antar *router* dan *switch.* Dan *slave port* berperan sebagai *access* port untuk mendistribusikan VLAN ke divisi.

Kemudian menkonfigurasi *switch mode* dan mengatur *ether1* sebagai *trunk port* dan *ether 2, 3, 4* sebagai *access port. Ether* 1 VLAN *Mode Secure* dan *add if missing* adalah paket yang masuk dengan VLAN TAG, lalu akan menambahkan VLAN *Header*. Ini yang disebut sebagai *trunk port.* Kemudian *ether 2, 3,* dan *4,* dengan VLAN *Header always strip* adalah paket yang keluar akan dihilangkan VLAN *Header nya* pada paket data.



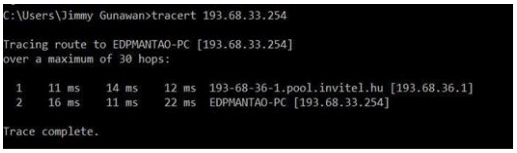
Gambar 5. *Switch Port VLAN*

Kemudian di gambar 5 akan terlihat paket data yang masuk dari *ether 1* yang bertindak sebagai *trunk* akan diselipkan VLAN *Header* ke *ether 2,* kemudian paket data yang keluar dari *ether 2* akan dihilangkan VLAN *Header* nya. Begitu pula dengan *ether 3* dan *ether 4.*

Hasil Ping bisa dilihat disini:

Gambar 6. Ping Sesama VLAN ID

Terlihat disini jika komputer melakukan PING sesama VLAN ID, maka jika di *traceroute* akan terlihat jalurnya langsung menuju tujuan.



Gambar 7. Ping Berbeda VLAN ID

Terlihat pada gambar 7 jika komputer melakukan PING antar komputer yang berbeda VLAN ID, maka jika di *traceroute* akan terlihat jalurnya menuju *gateway (router)* terlebih dahulu, lalu menuju komputer tujuan. Ini disebut berkomunikasi melalui *Inter-VLAN.*

Hasil *Bandwidth*

Penulis akan mencoba mengirim *file.* Penulis akan mengambil data di *server*. Penulis melakukan pengujian untuk mengetahui protokol SMB berjalan dan bisa di analisa *delay* nya. Penulis mengirim data yang berisi aplikasi sebesar 99. MB. Pada saat pengiriman, penulis merekam nya dengan aplikasi *bandwidth meter pro* dan *wireshark.*

Parameter *adapter* adalah *adapter* jaringan yang digunakan apakah *wireless* atau menggunakan kabel LAN. Disini penulis menggunakan *adapter Realtek,* yaitu menggunakan kabel LAN. Kemudian parameter total, total disini dimaksudkan adalah total jumlah data yang ditransmisikan, disini terlihat *164,32 MegaBytespersecond.* Yang dimaksud adalah data yang dikirim melewati kabel LAN sebesar *164,32 MegaBytespersecond.* Parameter *Maximum* dan *Minimum Rate* adalah maksimum dan minimum kecepatan transmisi data yang satuannya adalah *Mbitpersecond*. Maksimum kecepatannya adalah *25.7 Mbitpersecond*, minimum nya *992 bitpersecond.* Kemudian ada *average rate* yang artinya adalah rata-rata kecepatan pada saat transmisi data. Disini rata-rata kecepatannya adalah *13.4 Mbitpersecond.* Kemudian ada total waktu pada saat transmisi selesai yaitu 1 menit 43 detik. Yang artinya pengambilan data sebesar *164,32 MegaBytespersecond* membutuhkan waktu 1 menit 43 detik dengan kecepatan

Jurnal Algoritma, Logika dan Komputasi
Vol.II (No. 1) : 138 - 150. Th. 2019
p-ISSN: 2620-620X
e-ISSN: 2621-9840

maksimal *25.7 Mbitpersecond*, kecepatan minimum nya *992 bitpersecond*, rata-rata kecepatannya *13.4 Mbitpersecond.*

Dapat disimpulkan hasil penelitian dari 10 percobaan dalam bentuk tabel sebagai berikut:

Tabel 7. SMB

Percobaan download	1	2	3	4	5	6	7	8	9	10	Rata2
Max(Mbps)	25.7	26.3	26.1	25.3	25.7	25.2	25.7	26	26.2	26.5	25.87
Min(Mbps)	0.992	2	0.001	2.8	1.99	0.198	2.68	0.005	0.46	0.778	1.19
Average(Mbps)	13.4	13.5	12.2	17.1	16.3	16.4	13.9	16.3	18.3	15	15.24
Time (min:second)	01:43	01:42	01:53	01:20	01:19	01:53	01:38	01:44	01:30	01:33	01:37
Average Delay(ms)	234.3	231.8	228.6	203.2	170.8	180.7	236.1	186.2	143.1	188	200.28
Kategori	Bagus	Bagus	Bagus	Bagus	Bagus	Bagus	Bagus	Bagus	Sangat bagus	Bagus	Bagus

Disini terlihat tabel 7 adalah tabel rata-rata dari 10 pengujian yang menggunakan *protocol* SMB yang direkam menggunakan aplikasi *bandwidth meter pro* dan *wireshark* untuk merekam paket *delay*. Terlihat ada 10 percobaan ada parameter *max, min, average, time, average delay.*

Pada percobaan pertama terdapat maksimum kecepatan *25,7 Megabitpersecond*, minimal kecepatan *0,992 Megabitpersecond*, dan rata-rata kecepatan, *13,4 Megabitpersecond*, kemudian waktu yang dibutuhkan untuk transmisi data adalah 1 menit 43 detik yang memiliki rata-rata paket yang *delay 234,3 milisecond* yang terlihat di tabel 7 tertulis bahwa rata-rata paket *delay* dengan *234,3 milisecond* tergolong kategori bagus.

Pada percobaan kedua terdapat maksimum kecepatan *26.3 Megabitpersecond*, minimal kecepatan *2 Megabitpersecond*, dan rata-rata kecepatan, *13,5 Megabitpersecond*, kemudian waktu yang dibutuhkan untuk transmisi data adalah 1 menit 42 detik yang memiliki rata-rata paket yang *delay 231,8 milisecond* yang terlihat di tabel 7 tertulis bahwa rata-rata paket *delay* dengan *231,8 milisecond* tergolong kategori bagus.

Pada percobaan ketiga terdapat maksimum kecepatan *26.1 Megabitpersecond*, minimal kecepatan *0.001 Megabitpersecond*, dan rata-rata kecepatan, *12.2 Megabitpersecond*, kemudian waktu yang dibutuhkan untuk transmisi data adalah 1 menit 53 detik yang memiliki rata-rata paket yang *delay 228,8 milisecond* yang terlihat di tabel 7 tertulis bahwa rata-rata paket *delay* dengan *228,8 milisecond* tergolong kategori bagus.

Pada percobaan keempat terdapat maksimum kecepatan *25.3 Megabitpersecond*, minimal kecepatan *2.8 Megabitpersecond*, dan rata-rata kecepatan, *17,5 Megabitpersecond*, kemudian waktu yang dibutuhkan untuk transmisi data adalah 1 menit 20 detik yang memiliki rata-rata paket yang *delay 203,2 milisecond* yang terlihat di tabel 7 tertulis bahwa rata-rata paket *delay* dengan *203,8 milisecond* tergolong kategori bagus.

Pada percobaan kelima terdapat maksimum kecepatan *25.7 Megabitpersecond*, minimal kecepatan *2 Megabitpersecond*, dan rata-rata kecepatan, *16.3 Megabitpersecond*, kemudian waktu yang dibutuhkan untuk transmisi data adalah 1 menit 19 detik yang memiliki rata-rata paket yang *delay 170,8 milisecond* yang terlihat di tabel 7 tertulis bahwa rata-rata paket *delay* dengan *170,8 milisecond* tergolong kategori bagus.

Pada percobaan keenam terdapat maksimum kecepatan *26.2 Megabitpersecond*, minimal kecepatan *2 Megabitpersecond*, dan rata-rata kecepatan, *16,5 Megabitpersecond*, kemudian waktu yang dibutuhkan untuk transmisi data adalah 1 menit 53 detik yang memiliki rata-rata paket yang *delay 180,8 milisecond* yang terlihat di tabel 7 tertulis bahwa rata-rata paket *delay* dengan *180,8 milisecond* tergolong kategori bagus.

Pada percobaan ketujuh terdapat maksimum kecepatan *25.7 Megabitpersecond*, minimal kecepatan *2,68 Megabitpersecond*, dan rata-rata kecepatan, *13,9 Megabitpersecond*, kemudian waktu yang dibutuhkan untuk transmisi data adalah 1 menit 38 detik yang memiliki rata-rata paket yang *delay 236,8 milisecond* yang terlihat di tabel 2.1 tertulis bahwa rata-rata paket *delay* dengan *236,8 milisecond* tergolong kategori bagus.

Pada percobaan kedelapan terdapat maksimum kecepatan *26 Megabitpersecond*, minimal kecepatan *0,005 Megabitpersecond*, dan rata-rata

Jurnal Algoritma, Logika dan Komputasi
Vol.II (No. 1) : 138 - 150. Th. 2019
p-ISSN: 2620-620X
e-ISSN: 2621-9840

kecepatan, *16,3 Megabitpersecond*, kemudian waktu yang dibutuhkan untuk transmisi data adalah 1 menit 44 detik yang memiliki rata-rata paket yang *delay 186,2 milisecond* yang terlihat di tabel 7 tertulis bahwa rata-rata paket *delay* dengan *186,2 milisecond* tergolong kategori bagus.

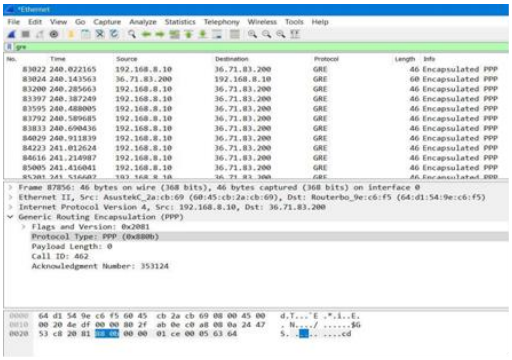
Pada percobaan kesembilan terdapat maksimum kecepatan *26.2 Megabitpersecond*, minimal kecepatan *0.46 Megabitpersecond*, dan rata-rata kecepatan, *18,3 Megabitpersecond*, kemudian waktu yang dibutuhkan untuk transmisi data adalah 1 menit 30 detik yang memiliki rata-rata paket yang *delay 143,1 milisecond* yang terlihat di tabel 7 tertulis bahwa rata-rata paket *delay* dengan *143,1 milisecond* tergolong kategori sangat bagus.

Pada percobaan kesepuluh terdapat maksimum kecepatan *26.5 Megabitpersecond*, minimal kecepatan *0,778 Megabitpersecond*, dan rata-rata kecepatan *15 Megabitpersecond*, kemudian waktu yang dibutuhkan untuk transmisi data adalah 1 menit 33 detik yang memiliki rata-rata paket yang *delay 188 milisecond* yang terlihat di tabel 7 tertulis bahwa rata-rata paket *delay* dengan *188 milisecond* tergolong kategori bagus.

Disni terlihat berbeda-beda pada setiap percobaan karena tergantung pada situasi dan kondisi cuaca atau masalah *signal* pada masing-masing ISP. Dan kemudian rata-rata dari kesepuluh percobaan ini terdapat kecepatan maksimum adalah *25,87 Megabitpersecond*, minimum *1,19 Megabitpersecond*, rata-rata kecepatan pada ke sepuluh percobaan adalah *15,24 Megabitpersecond*, dan waktu yang dibutuhkan untuk transmisi data adalah 1 menit 37 detik yang memiliki rata-rata paket *delay* sebesar *200,28 milisecond* dan rata-rata kategori pada kesepuluh percobaan adalah bagus.

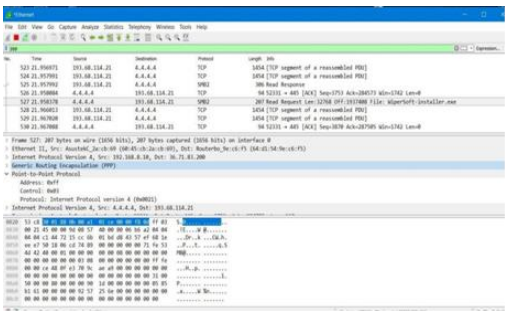
Hasil *Sniffing*

Berikut adalah hasil *sniffing* menggunakan aplikasi *wireshark* ke interface *tunnel* terlihat data dibungkus dengan protokol GRE yang sudah di enkapsulasi dengan PPP dan ada PPTP *header* yang dapat dilihat pada gambar 8 dan gambar 9:



Gambar 8. Hasil *Sniffing* 1

Gambar 8 terlihat protokol GRE yang membungkus paket untuk dikirimkan ke IP tujuan. Sehingga pada saat di *sniffing* data akan aman dan tidak terlihat oleh oknum lain.



Gambar 9. Hasil *Sniffing* 2

Gambar 9 pada saat di *sniffing* terlihat protokol SMB sedang berjalan untuk mengirimkan data dan data tersebut dibungkus oleh protokol GRE sehingga data akan aman sampai ke IP tujuan.

KESIMPULAN

Dengan penelitian ini maka penulis mendapatkan beberapa hasil kesimpulan:

1. Metode VPN *tunnel* PPTP dapat menghubungkan kantor pusat dengan kantor cabang dengan cara membuat terowongan pada jalur publik yang disertai enkripsi pada data yang ditransmisikan, sehingga keamanan data akan lebih terjamin.
2. Metode BCP *(Bridge Control Protocol)* yang diimplementasikan dalam metode *tunneling*, dapat menghubungkan

Jurnal Algoritma, Logika dan Komputasi
Vol.II (No. 1) : 138 - 150. Th. 2019
p-ISSN: 2620-620X
e-ISSN: 2621-9840

kantor pusat dengan kantor cabang menjadi 1 segmentasi yang sama.

3. Kantor cabang dapat mengolah data menggunakan *Microsoft Great Plains* pada kantor pusat menggunakan metode metode *tunneling* dan BCP dengan aman.

DAFTAR PUSTAKA

[1] Nugroho, Irwan, et al, 2014. Perbandingan performansi jaringan *Virtual Private Network* metode *Point* to *Point Tunneling Protocol* (PPTP) dengan metode *Internet Protocol Security*. ISSN:2338-4018. *TIKomSiN*.

[2] Pratama, 2015. *Handbook* Jaringan Komputer.

[3] Mufida, Elly, et al, 2017. *Remote Site* Mikrotik VPN dengan *Point to Point Tunneling* Protocol (PPTP) studi kasus pada Yayasan Teratai Global Jakarta. ISSN:1858-4144. *MATRIK*, 10.

[4] Septiardi, Vidi Dwi, 2017. Membangun Jaringan Intranet dengan melewatkan VLAN diatas VPN menggunakan metode PPTP BCP.

[5] Hermawan, Rian Heri & Bobi Kurniawan, 2015. Implementasi *Ethernet Over* IP *File* Mikrotik *Router* Os pada layanan *Voice Over* IP di PT Akurasi Kuat Mega. ISSN:2089-9033. KOMPUTA