MEMBANGUN JARINGAN INTRANET DENGAN MELEWATKAN VLAN DIATAS VPN MENGGUNAKAN METODE PPTP BCP

Vidi Dwi Septiardi
D3 Manajemen Informatika, Fakultas Teknik, Universitas Negeri Surabaya, vidivido76@gmail.com

Agus Prihanto
Jurusan Teknik Informatika, Fakultas Teknik, Universitas Negeri Surabaya, agusprihanto@unesa.ac.id

Abstrak

Internet sudah menjadi kebutuhan wajib bagi organisasi atau perkantoran, Terutama kantor yang memiliki cabang yang jaraknya jauh dengan kantor pusat. Untuk menghubungkan antar perusahaan yang saling berjauhan agar tetap dapat bertukar informasi atau data bisa menyewa *leased line* namun memerlukan biaya yang cukup mahal.

Dari permasalahan tersebut penulis memunculkan gagasan memanfaatkan tunneling diatas internet. Internet merupakan jaringan publik yang telah tersebar luas dan mendunia sehingga dapat digunakan dengan mudah. Sebuah teknologi komunikasi *Virtual Private Network* yang memungkinkan jaringan komputer dimana antar perangkatnya terhubung memanfaatkan jaringan publik(internet) sehingga diperlukan koneksi internet pada masing-masing kantor pusat dan cabang. Setiap kantor pusat dan cabang memiliki 3 departement yang berbeda. Setiap departement nantinya akan di pisah menjadi beberapa segment seperti departement admin dengan departement admin saja yang dapat terhubung. Untuk itu dapat menggunakan metode *Bridge Control Protocol* yang memungkinkan untuk meneruskan paket melalui tunneling *Point-to-Point Tunneling Protocol*(PPTP) dan untuk memisahkan departement antar kantor pusat dan cabang dapat menggunakan jaringan *Virtual Local Area Network*(VLAN) yang nantinya setiap departement diberikan identitas(ID) sesuai dengan departement yang ada pada kantor pusat dan cabang.

Hasil dari penelitian menunjukkan bahwa dengan adanya internet yang terhubung pada setiap kantor pusat dan cabang dapat dimanfaatkan sebagai media penghubung untuk membentuk koneksi tunnel VPN. Setelah VPN tunnel terbentuk, rute yang dilalui antara kantor pusat dengan kantor cabang seperti berada pada satu jaringan LAN yang sama dan juga dengan menggunakan metode VLAN dapat membuat segment jaringan lebih kecil seperti halnya sesama departement dapat saling terhubung dan jika berbeda departement ingin saling terhubung maka kedua departement yang berbeda tersebut harus menggunakan *default gateway* yang menuju ke router kantor masing-masing departement.
Kata kunci : Virtual Private Network, Virtual Local Area Network, Point-to-Point Tunnel Protocol, Bridge Control Protocol.

Abstract

The Internet has become a mandatory requirement for organizations or offices, especially the office which has branches located in remote areas with the headquarters. To connect with companies that are further apart in order to remain able to exchange information or data can be rented leased line but the cost quite expensive.

From these problems, the authors raise the idea of utilizing the tunneling over the internet. The Internet is a public network that is already widespread and worldwide so that it can be used easily. A communication technology Virtual Private Network that enables a computer network where the device is connected between utilizing public network (Internet) so that the internet connection is required in each central office and branches. Each branch has its headquarters and three different departments. Each department will be split into several segments such as department admin with the admin department that can be connected. For it can use the method of Bridge Control Protocol, which allows it to forward packets via tunneling Point-To-point Tunneling Protocol(PPTP) and to separate the department between headquarters and branch offices can use the network of Virtual Local Area Network(VLAN), which will each department is given the identity (ID) in accordance with existing department at the head office and branches.

Results from the study showed that the presence of a VPN with PPTP BCP showed that after the PING between routers branches and the central router connection can run smoothly and after testing traceroute shows the route is shorter compared to before the establishment of the VPN tunnel and also the results of testing of sharing files above VLAN indicates that each department would only be sharing files between one department, so that the isolation between departments can be maintained. For cross-linking the department should be made inter-VLAN routing that links the department.
Keywords: Virtual Private Network, Virtual Local Area Network, Point-to-Point Tunnel Protocol, Bridge Control Protocol.

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. Setiap kantor pusat dan cabang memiliki 3 departement yang berbeda. Setiap departement nantinya akan dipisah menjadi beberapa segment seperti departement Admin kantor pusat dengan departement Admin kantor cabang yang saling terhubung dengan satu segment. Untuk itu dapat menggunakan metode *Bridge Contorl Protocol* yang memungkinkan meneruskan paket melalui tunneling *Point-to-Point Tunneling Protocol*(PPTP) dan untuk memisahkan departement antar kantor pusat dengan departement kantor cabang dapat menggunakan jaringan *Virutal Local Area Network*(VLAN) yang nantinya setiap departement diberikan Identitas(ID) sesuai dengan departement pada kantor pusat dan cabang.

Internet merupakan hal penting untuk membangun sebuah jaringan VPN karena internet dimanfaatkan sebagai media penghubung untuk membentuk koneksi tunnel VPN. Setelah VPN terbentuk, rute yang dilalui antar kantor pusat menuju kantor cabang menjadi lebih pendek karena jaringan antar kantor pusat dan cabang akan seperti berada pada satu jaringan LAN yang sama dan juga dengan menggunakan metode VLAN dapat membuat segment jaringan lebih kecil seperti halnya sesama departement dapat saling terhubung, jika berbeda departement ingin saling terhubung maka kedua departement yang berbeda tersebut harus menggunakan *default gateway* yang menuju ke router kantor masing-masing departement.

KAJIAN PUSTAKA

Jaringan Intranet

intranet adalah sebuah jaringan komputer yang saling terhubung atau tersambung yang digunakan oleh suatu sistem organisasi maupun lembaga. Intranet merupakan suatu jaringan komputer yang berbasis protokol TCP/IP, layaknya jaringan internet namun penggunanya yang dibatasi atau lebih tertutup jadi tidak semua pengguna atau orang dapat secara mudah mengakses jaringan intranet serta hanya orang atau pengguna tertentu saja yang dapat masuk dan menggunakan jaringan intranet.

Open Shortest Path First

Open Shortest Path First adalah sebuah *protocol routing* otomatis (*Dynamic Routing*) yang mampu menjaga, mengatur dan mendistribusikan informasi antar network mengikuti setiap perubahan jaringan secara dinamis. Pada OSPF dikenal sebuah istilah *autonomus system* (AS) yaitu sebuah gabungan dari beberapa jaringan yang sifatnya *routing* dan memiliki kesamaan metode serta *policy* pengaturan *network*, yang semuanya dapat dikendalikan oleh *network administrator*. Dan memang kebanyakan fitur ini digunakan untuk management dalam skala jaringan yang sangat besar. Oleh karena itu untuk mempermudah penambahan informasi *routing* dan meminimalisir kesalahan distribusi informasi *routing*, maka OSPF bisa menjadi sebuah solusi. OSPF termasuk di dalam katagori IGP (*Interior Gateway Protocol*) yang memiliki kemampuan *Link-State* dan algoritma Djikstra yang jauh lebih efisien dibandingkan protocol IGP yang lain. Dalam operasinya OSPF menggunakan protokol sendiri yaitu protocol 89. OSPF merupakan protokol routing yang menggunakan konsep hirarki routing, dengan kata lain OSPF mampu membagi-bagi jaringan menjadi beberapa tingkatan-tingkatan ini diwujudkan dengan menggunakan sistem pengelompokan yaitu area.

Virtual Local Area Network

Prinsip kerja sebuah jaringan LAN(*Local Area Network)* semua *device* yang berada pada satu LAN berarti berada pada satu *broadcast domain.* Sebuah

broadcast domain mencakup semua device yang terhubung pada satu LAN dimana jika salah satu *device* mengirimkan *frame broadcast* maka semua *device* yang lain akan menerima kopi dari *frame* tersebut. Tanpa VLAN, sebuah switch akan menganggap semua *interface* (*port*) nya berada pada satu broadcast domain, dengan kata lain semua komputer yang terhubung ke switch tersebut akan akan dianggap berada pada satu LAN yang sama. Dengan menggunakan teknologi VLAN, switch bisa mengelompokkan beberapa *interface* yang lain kedalam *broadcast domain*. Masing-masing *broadcast domain* yang dibuat oleh switch inilah yang disebut sebagai *Virtual Local Area Network*(VLAN)

Virtual Private Network

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada didalam jaringan LAN yang sama, walaupun sebenarnya menggunakan jaringan milik publik.

VPN dapat dibentuk dengan menggunakan teknologi *tunneling* dan enkripsi. Koneksi VPN juga dapat terjadi pada semua layer pada protokol OSI, sehingga komunikasi menggunakan VPN dapat digunakan berbagai perlu.

Point-to-Point Tunneling Protocol

Point-to-Point Tunneling Protocol (PPTP) merupakan protokol jaringan yang memungkinkan pengamanan *transfer* data *remote client* ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP.

Teknologi jaringan PPTP merupakan pengembangan dari *remote access Point-to-Point Tunneling Protocol* yang dikeluarkan oleh *Internet Engineering Task Force*(IETF). PPTP merupakan protokol jaringan yang merubah paket PPP menjadi IP *datagrams* agar dapat di transmisikan melalui internet.PPTP juga dapat digunakan pada jaringan *private LAN-to-LAN*.

Bridge Control Protocol

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.

METODE

Analisa Sistem

Analisa sistem yang akan dirancang adalah membangun jaringan intranet dengan melewatkan VLAN diatas VPN menggunakan metode PPTP BCP pada router Mikrotik.

Untuk membangun sebuah infrastruktur jaringan antar kota yang saling berjauhan cukup memakan biaya yang sangat mahal karena membutuhkan banyak alat dan bahan yang digunakan yaitu switch hub, router, access point, dan RJ-45 beserta kabel UTP perroll yaitu 305m maka memerlukan 28.975 roll untuk menyambungkan antar kantor pusat yang berada di Surabaya dan kantor cabang yang berada di Malang. estimasi biaya untuk membangun jaringan antar 2 kota sebagai berikut:

Tabel 1 anggaran dana jaringan antar kota

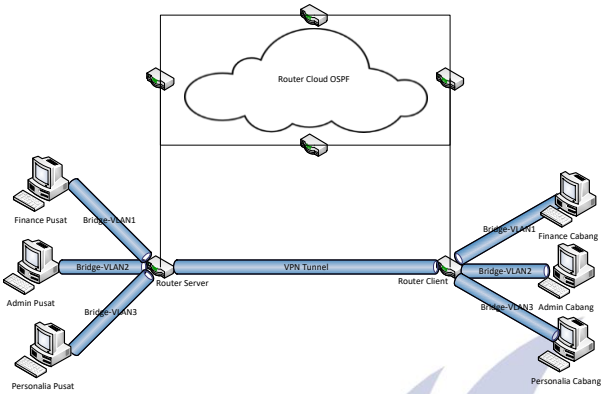
Alat	Type	Harga	qty	total
Switch hub	D-LINK DGS-1024	Rp 1,299.00	2	Rp 2,580,000
Access Point	LINKSYS WIRELESS N300 WITH POE	Rp 1,949,000	2	Rp 3,898,000
Kabel UPT	-	Rp 100,000	28.975roll	Rp 2,897,500,000
Konektor RJ-45	-	Rp 50,000	1	Rp 50,000
Router	RB1100Ahx2 1U	Rp 4,727,000	2	Rp 9,454,000
Total				Rp 2,913,482,000

Adapun perbandingan biaya yaitu menggunakan jasa leased line yang dapat dibandingkan dengan estimasi biaya sewa perbulan Rp. 750.000 dan biaya setup sampai dengan Rp. 4.500.000. Untuk menghemat biaya yang akan digunakan untuk infrastruktur jaringan antar 2 kota, maka penulis pada tugas akhir ini membangun jaringan intranet sebagai solusi mengatasi mahalnya untuk membangun jaringan antar 2 kota.

Untuk menghubungkan antar 2 kantor yang saling berjauhan membutuhkan koneksi *Virtual Private Network* (VPN) yang nantinya koneksi antar kantor akan menggunakan teknologi *tunneling*. Untuk membuat sebuah *tunneling*, maka setiap kantor harus terhubung ke internet. *service* yang biasa digunakan untuk membangun *tunnel* VPN yaitu *Point-to-Point Tunneling Protocol* (PPTP). Sebuah koneksi PPTP terdiri dari *server* dan *client*. Untuk memenuhi kebutuhan agar kedua kantor dapat menggunakan IP *segment* yang sama dibutuhkan metode *bridging*. Sehingga dalam jaringan ini menggunakan kombinasi metode *Point-to-Point Tunneling Protocol* dan *Bridge Control Protocol*. Untuk

membuat jaringan menjadi flexsibel dimana dapat dibuat *segment* yang hanya bergantung pada setiap departement antar kantor saja maka dibuat VLAN diatas VPN.

Desain Topologi



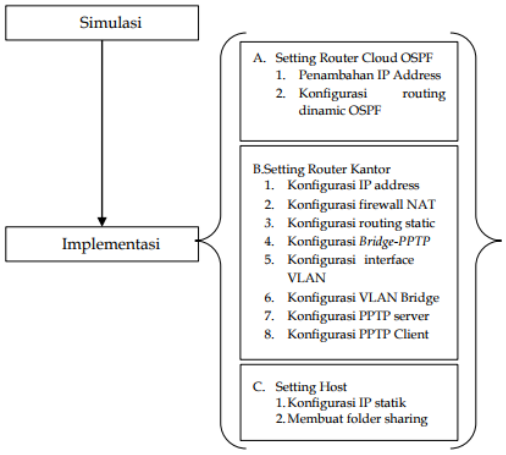
Gambar 1 Desain Topologi

Dalam proposal tugas akhir ini, penulis membangun jaringan intranet dengan melewatkan VLAN diatas VPN menggunakan metode PPTP BCP.

Pada gambar 1 terdapat 2 kantor yaitu kantor Pusat Dan Kantor Cabang, Setiap Kantor Memiliki 3 departement. Setiap router kantor saling terhubung ke internet dengan menggunakan 4 router sebagai *cloud OSPF*.

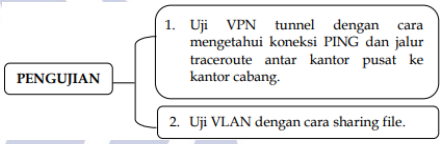
Untuk menghubungkan antar 2 kantor yang saling berjauhan, maka setiap router kantor harus terhubung ke internet sebagai media perantaranya seperti pada gambar 1 masing-masing router kantor pusat dan cabang terhubung ke internet. Jika sudah terhubung ke internet maka *tunnel Virtual Private Network* (VPN) dapat terbentuk. *service* yang digunakan untuk membangun koneksi *tunnel* VPN yaitu *Point-To-Point Tunneling Protocol* (PPTP). Sebuah protokol jaringan PPTP terdiri dari *server* dan *client* dimana kantor pusat sebagai *server* dan kantor cabang sebagai *client.* Untuk memenuhi kebutuhan agar kedua kantor dapat menggunakan IP *segment* yang sama dibutuhkan metode *bridging*. Sehingga dalam jaringan ini menggunakan kombinasi *Point-To-Point Tunneling Protocol* dan *Bridge Control Protocol.* Untuk membuat jaringan menjadi *flexibel* dimana dapat dibuat segment yang hanya bergantung pada sesama departement antar 2 kantor dengan melewatkan VLAN diatas VPN maka setiap departement diberikan VLAN ID yang sesaui dengan departement antar kantor pusat dan cabang.

Perancangan Sistem



Gambar 2 Perancangan Sistem

Skenario Pengujian



Gambar 3 Skenario Pengujian

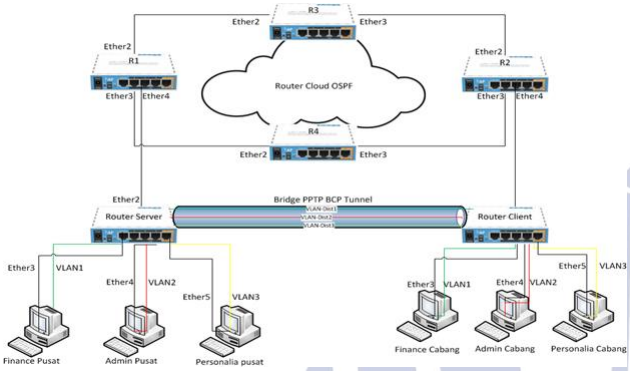
Skenario pengujian sebagai tahap menganalisa hasil dari uji coba. Tahapan pengujian penelitian sebagai berikut:

1. Melakukan pengujian test koneksi PING dan rute sebelum ada koneksi VPN tunnel yang mana bila dilakukan traceroute antar kantor cabang menuju kantor pusat untuk mengetahui rute yang dilewati paket untuk mencapai tujuan.
2. Melakukan uji VLAN dengan cara melakukan sharing file antar antar departement yang sama dan dengan berbeda departement

HASIL DAN PEMBAHASAN

Penelitaian ini bertujuan untuk membangun jaringan intranet dengan melewatkan VLAN diatas VPN menggunakan metode PPTP BCP. sebelum melakukan implementasi penulis melakukan simulasi pada GNS3 untuk mempermudah saat proses implementasi. Untuk menghubungkan antara dua kantor yang saling berjauhan maka dibangun sebuah VPN. Setiap router yang ada pada kantor pusat dan cabang harus terhubung pada *internet* sebagai media perantara agar VPN dapat terbentuk. Salah satu *service* untuk membangun VPN adalah PPTP yang terdiri dari *server* dan *client* dalam hal ini kantor pusat sebagai *server* dan kantor cabang sebagai *client.* Ketika PPTP sudah terbentuk maka *interface* PPTP akan secara otomatis menjadi *bridge port* pada Bridge-PPTP hal ini disebut dengan metode *bridging* atau *Bridge Control Protocol*(BCP). Pada Bridge-PPTP akan digunakan untuk mendistribusikan VLAN antara kantor pusat dan kantor cabang melalui VPN *tunnel.* Untuk memenuhi kebutuhan agar kedua departement yang ada pada kantor pusat dan

cabang saling terhubung dengan *segment* IP yang sama maka dibuatkan VLAN *Bridge* yang nantinya VLAN utama dan *ether* yang langsung terhubung pada departement dijadikan sebagai *ports* pada *interface bridge-vlan* dan ditentukankan identitas(ID) sesuai dengan departementnya dengan begitu jika berbeda departement ingin bertukar data harus menggunakan *default gateway* router kantor masing-masing departement. Berikut gambar 4 adalah topologi jaringan yang digunakan :



Gambar 4 Tologi Jaringan

Berikut adalah hasil setting yang dilakukan :

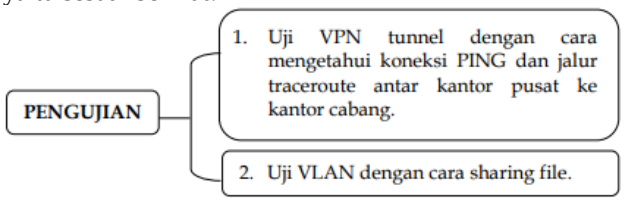
1. Setting router cloud OSPF
   a) Konfigurasi IP address
   b) Konfigurasi routing dinamik OSPF

2. Setting Router Kantor
   a) Konfigurasi IP address
   b) Konfigurasi firewall NAT
   c) Konfigurasi routing statik
   d) Konfigurasi Bridge-PPTP
   e) Konfigurasi interface VLAN
   f) Konfigurasi VLAN Bridge
   g) Konfigurasi PPTP Server
   h) Konfigurasi PPTP client

3. Setting host(Departement)
   a) Konfigurasi IP statik
   b) Membuat folder sharing

Pengujian dan Pembahasan

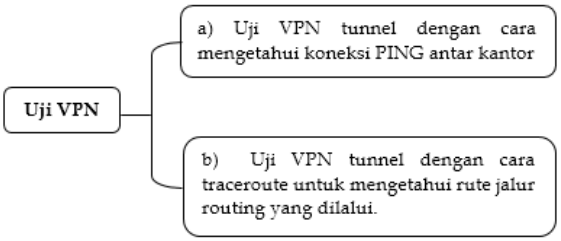
Pengujian yang dilakukan yaitu sesuai dengan skenario pengujian yang sudah dibuat pada tahap sebelumnya yaitu sesuai berikut:



Gambar 5 Pengujian

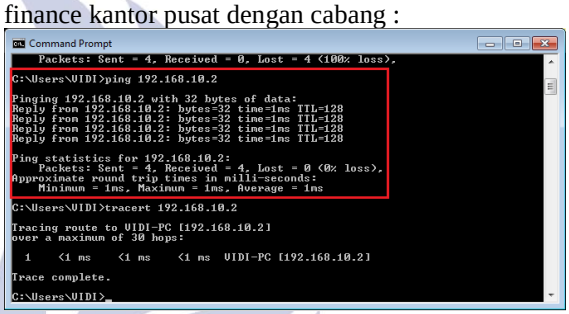
1. Pengujian yang pertama dilakukan yaitu uji VPN tunnel dengan cara mengetahui koneksi PING dan jalur traceroute antar kantor pusat ke kantor cabang.

Berikut adalah hasil uji coba yang telah penulis lakukan :



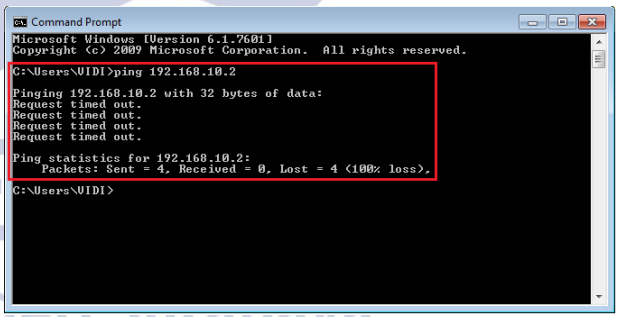
Gambar 6 Uji VPN

a) Uji VPN tunnel dengan cara test koneksi PING yang dilakukan pada host(departement) yang ada pada setiap kantor hal ini dilakukan agar mengetahui tunnel VPN sudah berhasil terhubung atau tidak. Berikut adalah hasil uji VPN tunnel dengan cara test koneksi PING antara departement finance kantor pusat dengan cabang :



Gambar 7 hasil tes koneksi PING sesama departement sesudah tunnel terbentuk

Pada gambar 7 Hasil test koneksi PING berhasil terhubung antar kantor pusat dengan kantor cabang dan sudah dapat saling bertukar data.

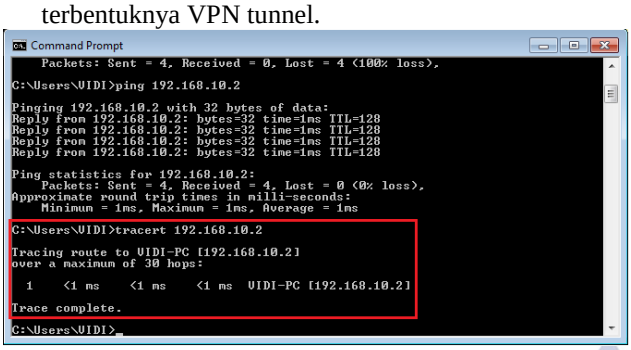


Gambar 8 hasil tes koneksi PING sesama departement sebelum tunnel terbentuk

Pada gambar 8 Sebelum terbentuknya VPN *tunnel* koneksi antar kantor pusat dengan kantor cabang tidak dapat terhubung karena kantor pusat dan kantor cabang sama-sama tehubung pada internet. Koneksi internet tidak dapat meneruskan paket dikarenakan antar komputer yang terhubung dengan koneksi internet menggunakan IP lokal atau dengan kata lain internet tidak bisa mengenal IP lokal yang digunakan antar komputer.

b) Uji traceroute VPN *tunnel* untuk mengetahui jalur routing yang dilalui. Berikut adalah beberapa hasil uji *traceroute* yang dilakukan :

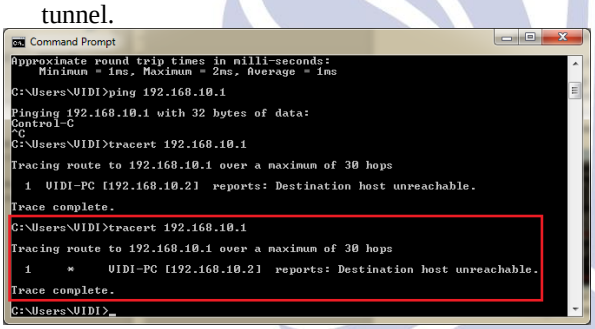
1) Uji traceroute sesama departement setelah terbentuknya VPN tunnel.



Gambar 9 Uji traceroute sesama departement setelah terbentuknya tunnel

Hasil uji coba *tracert*(traceroute) yang didapatkan pada gambar 9 Menunjukkan bahwa jaringan antar kantor pusat dan kantor cabang seperti berada pada satu jaringan LAN yang sama hal ini dikarenakan hasil konfigurasi metode *Bridge Control Protocol.*

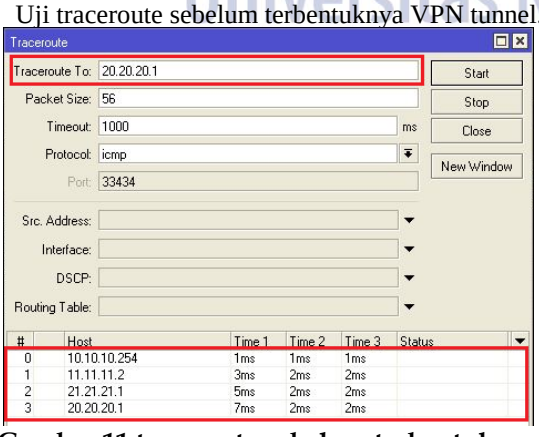
2) Uji traceroute sesama departement tanpa VPN tunnel.



Gambar 10 uji traceroute sesama departement tanpa Tunnel

Hasil uji *tracert*(traceroute) tanpa menggunakan tunnel VPN yang didapatkan pada gambar 10 Menunjukkan bahwa jaringan antar kantor pusat dan kantor cabang tidak dapat terhubung karena jaringan publik(internet) tidak dapat mengenali IP *private*

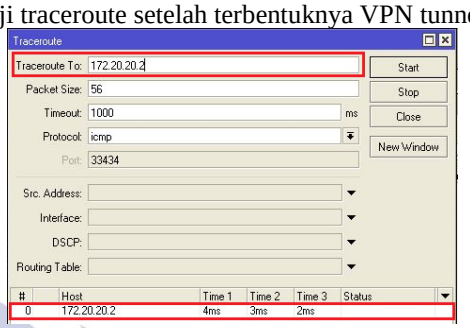
3) Uji traceroute sebelum terbentuknya VPN tunnel.



Gambar 11 traceroute sebelum terbentuknya VPN antar router server dan client

Hasil pada gambar 11 menunjukkan hasil *traceroute* sebelum terbentuknya VPN tunnel yaitu menggunakan *IP Public* router *server* menuju *IP Public* router *client* dan hasil rute yang diperoleh yaitu melalui router *cloud* OSPF terlebih dahulu sebelum sampai pada tujuan.

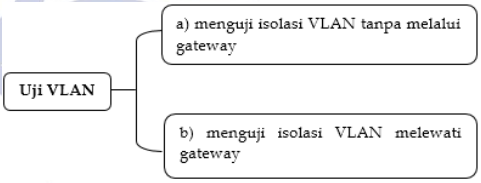
4) Uji traceroute setelah terbentuknya VPN tunnel.



Gambar 12 uji traceroute setelah terbentuknya VPN tunnel

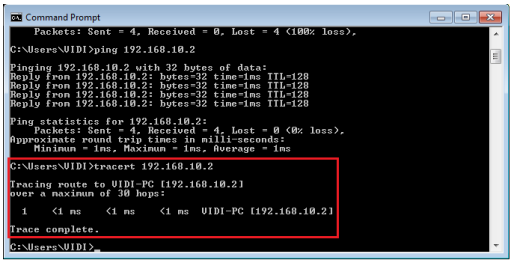
Hasil pada gambar 12 menunjukkan hasil *traceroute* setelah terbentuknya VPN tunnel. Uji *traceroute* yaitu menggunakan IP *tunnel* yang didapatkan masing-masing router kantor. Hasil rute yang diperoleh antara router server dan client yaitu menjadi lebih pendek jika dibandingkan sebelum terbentuknya VPN tunnel.

2. Pengujian yang kedua yaitu uji VLAN dengan cara melakukan sharing file antar departement. Sebelum melakukan uji coba sharing file dilakukan, penulis menguji isolasi VLAN tanpa melalui router dan melewati router seperti pada uji coba berikut:



Gambar 13 uji VLAN

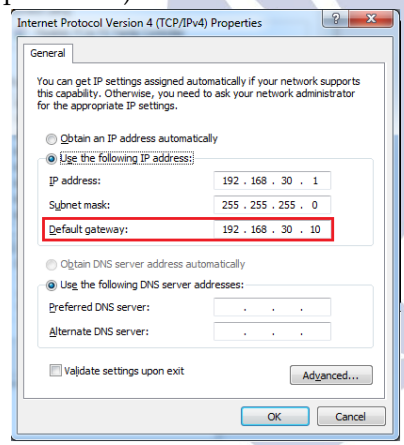
a) Pengujian yang pertama isolasi VLAN tanpa melalui gateway dengan cara traceroute untuk mengetahui rute yang dilalui untuk sampai pada tujuan. Berikut adalah hasil uji isolasi VLAN tanpa melalui router antara depertemen finance kantor pusat dengan departement finance kantor cabang:



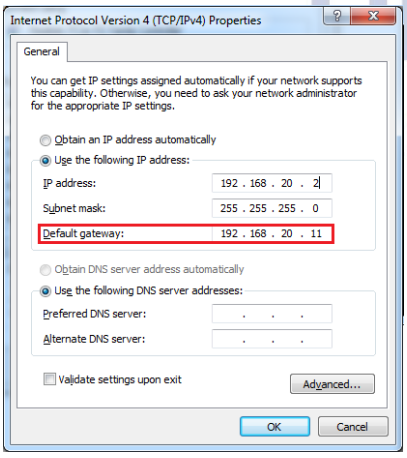
Gambar 14 Uji traceroute VLAN tanpa melalui gateway

Hasil pengujian pada gambar 14 terlihat rute yang dilalui departement finance kantor pusat menuju departement finance kantor cabang seperti pada jaringan LAN yang sama

b) Pengujian yang kedua isolasi VLAN melalui *gateway* dengan cara traceroute untuk mengetahui rute yang dilalui untuk sampai pada tujuan. Agar rute yang diambil melalui *gateway* terlebih dahulu maka pada host(departement) diberikan *default gateway* yang langsung menuju pada router masing-masing kantor hal ini juga dapat menghubungkan berbeda departement antar kantor pusat dengan cabang yang juga diberikan *default gateway* menuju router masing-masing host(departement). Berikut adalah cara memberi *default gateway* secara statik pada host(departement):

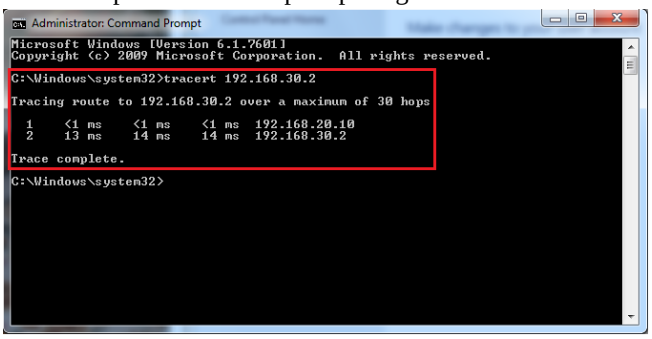


Gambar 15 default gateway server



Gambar 16 default gateway client

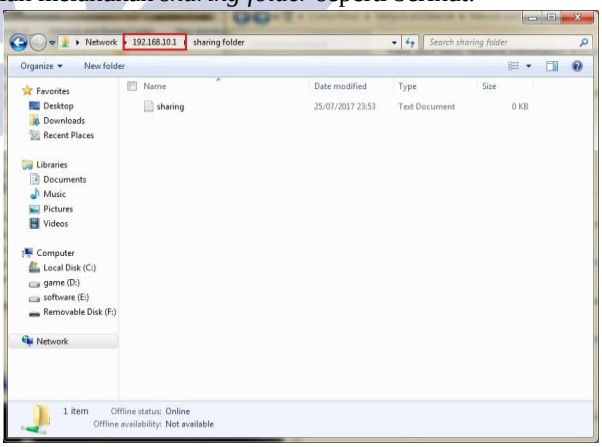
Jika *default gateway* masing-masing host(departement) sudah terpasang maka pengujian *traceroute* antara departement admin kantor pusat menuju departement finance dapat dilakukan seperti pada gambar 17 dibawah:



Gambar 17 Uji traceroute VLAN melalui gateway

Pada gambar 4.61 terlihat hasil *tracert*(*traceroute*) sebelum sampai tujuan IP 192.168.30.2 (departement personalia) yaitu melalui IP 192.168.20.10 yang mana IP tersebut adalah IP milik router kantor pusat departement admin

Jika koneksi kedua departement kantor pusat dan kantor cabang saling terhubung maka uji coba sharing folder dapat dilakukan. Departement finance pusat melakukan sharing *folder* yang didalamnya berisi *file* pada departement finance cabang dan departement finance cabang juga dapat menaruh dan mengedit *file* yang ada pada *folder* yang telah di *share* pada departement finance pusat dengan cara tekan **CTRL+R** lalu isikan IP **\\192.168.10.1** yaitu IP departement finance pusat yang telah melakukan *sharing folder* seperti berikut:



Gambar 18 Pengujian Sharing folder

Uji coba *sharing folder* berhasil dilakukan.

PENUTUP

Kesimpulan

Adapun kesimpulan yang didapatkan dari dua pengujian yaitu:

1. Hasil pengujian VPN dengan PPTP BCP menunjukan bahwa setelah dilakukan PING antar router cabang dan router pusat koneksi dapat berjalan lancar dan setelah dilakukan pengujian *traceroute* menunjukan

route yang lebih pendek jika dibandingkan dengan sebelum terbentuknya VPN *tunnel*.

2. Hasil pengujian *sharing file* di atas VLAN menunjukan bahwa setiap departement akan hanya dapat *sharing file* antar satu departement saja, sehingga isolasi antar departement dapat terjaga. Untuk menghubungkan lintas departement harus dibuatkan *routing* yang menghubungkan VLAN antar departement tersebut.

Saran

Pada penelitian selanjutnya diharapkan untuk menggunakan tunnel VPN yang berbeda tentunya seperti L2TP, EoIP, OVPN, SSTP. Dengan adanya opsi tersebut penulis berharap pengembang dapat memperluas jaringan dengan menggunakan lebih dari dua jaringan komputer antar kota.

DAFTAR PUSTAKA

Athailah. (2012). *Buku Pintar Ubuntu.* Jakarta Selatan: Mediakita.

Dewannanta, D. (2013, 1 29). *GNS3, Simulator Jaringan Komputer*. Diambil kembali dari Ilmu Komputer: http://ilmukomputer.org/2013/01/29/gns3/

huda, n. (2012, Juni 11). *Traceroute (Tracert)*. Diambil kembali dari rumahweb: www.rumahweb.com/journal/traceroute-tracert.html

huda, n. (2014, januari 20). *Perintah PING*. Diambil kembali dari rumahweb: www.rumahweb.com/journal/ping-domain.html

Kristanto, A. (2003). *Jaringan Komputer*. Yogyakarta: Graha Ilmu.

Nikko, S. (2014, 09 03). *Pengertian Internet dan Intranet lengkap dengan fungsinya*. Diambil kembali dari pengertianku: http://www.pengertianku.net/2014/09/pengertian-internet-dan-intranet-lengkap-dengan-fungsinya.html

Plimbi, E. (2011, 11 18). *Ketahui Perbedaan Jaringan VLAN vs LAN*. Diambil kembali dari Plimbi: http://www.plimbi.com/article/3357/ketahui-perbedaan-jaringan-vlan-vs-lan

Pratama, D. E. (2015). *Simulasi Office to Office Tunneling Dengan Metode PPTP Untuk Server Dan Bandwidth Management Untuk Client*.

Prihanto, A. (2015). Modul Jaringan Komputer. *Modul praktikum Jaringan Komputer*, 133.

Prihanto, A. (2015). Modul Jaringan Komputer. *Modul Praktikum Jarkom*, 134.

Prihanto, A. (2015). Modul Jaringan Komputer. *Modul Praktikum Jarkom*, 167.

Rohiman, A. (2011, 5 22). *Pengertian Routing, Tabel Routing dan Protocol Routing*. Diambil kembali dari catatan teknisi: http://www.catatanteknisi.com/2011/05/pengertian-routing-tabel-routing.html

Web, C. (2010, September 21). *Pemilihan Tipe VPN*. Diambil kembali dari mikrotik: www.mikrotik.co.id/artikel_lihat.php?id=61

Web, C. (2011, Agustus 4). *Konfigurasi Dasar OSPF*. Diambil kembali dari mikrotik: http://mikrotik.co.id/artikel_lihat.php?id=154

Web, C. (2012, Juli 19). *PPP Tunnel Bridging*. Diambil kembali dari mikrotik: www.mikrotik.co.id/artikel_lihat.php?id=97