

PERANCANGAN DAN SIMULASI AKSES JARAK JAUH MENGUNAKAN TEKNOLOGI VPN (STUDI KASUS KANTOR DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL TABALONG)

Rizkyka Angellia¹, Catur Iswahyudi², Prita Haryani³

¹Program Studi Informatika, Universitas AKPRIND Indonesia
Jl Kalisahak No. 28 Komplek Balapan Tromol Pos 45, Yogyakarta 55222 Telp : (0274) 563029
Email: rizkakyka02@gmail.com, catur@akprind.ac.id, pritaharyani@akprind.ac.id

Abstract

Cybersecurity is a very important thing to pay attention to, although sometimes some organizations prioritize appearance and other security issues, and when the system is hacked and the system crashes, the problems and losses will be greater. The Tabalong Population and Civil Registration Service Office is a government agency located in Tabalong Regency, South Kalimantan. Currently, the official office does not have a fast and stable internet connection for sending confidential data. As is generally known, the population and civil registration office has the task of carrying out population administration affairs in the field of Population and Civil Registration based on the Principle of Autonomy and Assistance Duties. The development of telecommunications networks is increasing. This is characterized by the emergence of various types of network technology available to companies and the public. Of course, the quality of the network technology provided must be of high quality, so that it can increasingly meet the needs of companies and society. The development of communication technology and network infrastructure continues to be developed following the Internetworking network which is currently increasingly developing. Cisco is the main equipment that is widely used in Wide Area Networks (WAN). With a Cisco router, information can be forwarded to addresses that are far apart and located on different computer networks. The location of this research was carried out at the Tabalong Regency Population and Civil Registration Office, Jl. H. Obar Sobari, Tabalong district, South Kalimantan, the VPN network provides more guaranteed security because it uses an authentication system with different user names and passwords for each user. With the VPN network, service or services available at the Tabalong Population and Civil Registration Office can run according to expectations and achieve its goals

Keywords: Telecommunication; VPN, Cisco; Network

Abstrak

Keamanan siber adalah hal yang sangat penting untuk diperhatikan, walaupun terkadang beberapa organisasi memprioritaskan penampilan dan lain-lain, masalah keamanan, dan ketika sistem diretas dan sistem crash, masalah dan kerugian akan lebih besar. Kantor Dinas Kependudukan dan Pencatatan Sipil Tabalong merupakan salah satu instansi pemerintahan yang berletak di Kabupaten Tabalong, Kalimantan Selatan. Saat ini kantor dinas tersebut belum memiliki jalur koneksi internet yang cepat dan stabil untuk pengiriman data yang bersifat rahasia. Seperti yang sudah umum diketahui bahwa kantor dinas kependudukan dan pencatatan sipil mempunyai tugas melaksanakan urusan administrasi kependudukan di bidang Kependudukan dan Pencatatan Sipil berdasarkan Azas Otonomi dan Tugas Pembantuan.

Perkembangan jaringan telekomunikasi semakin meningkat. Hal ini ditandai dengan munculnya berbagai jenis teknologi jaringan yang tersedia bagi perusahaan maupun publik. Tentunya kualitas dari teknologi jaringan yang disediakan harus berkualitas tinggi, sehingga semakin dapat memenuhi kebutuhan perusahaan dan masyarakat. Perkembangan teknologi komunikasi dan infrastruktur jaringan terus dikembangkan mengikuti jaringan Internetworking yang saat ini semakin berkembang, Cisco adalah peralatan utama yang banyak digunakan pada Jaringan Area Luas atau Wide Area

Network (WAN). Dengan cisco router, informasi dapat diteruskan ke alamat-alamat yang berjauhan dan berada di jaringan computer yang berlainan lokasi penelitian ini dilakukan di Kantor Dinas Kependudukan Dan Pencatatan Sipil Kabupaten Tabalong Jl. H. Obar Sobari kab Tabalong Kalimantan Selatan, Jaringan VPN memberikan kemanan lebih terjamin karena menggunakan sistem autentikasi pada user name dan password yang berbeda pada setiap user. Dengan adanya jaringan VPN, service atau layanan-layanan yang ada di Kantor Dinas Kependudukan Dan Pencatatan Sipil Tabalong bisa berjalan sesuai harapan dan tercapai tujuannya.

Kata kunci: Telekomunikasi; VPN; Cisco; Jaringan.

Pendahuluan

Saat ini, kemajuan dalam jaringan telekomunikasi terus meningkat. Hal ini termanifestasi melalui kemunculan berbagai macam teknologi jaringan yang tersedia untuk keperluan perusahaan dan masyarakat umum. Kualitas teknologi jaringan yang disajikan harus tetap tinggi agar dapat memenuhi kebutuhan dengan lebih baik. Perkembangan dalam teknologi komunikasi dan infrastruktur jaringan terus diupayakan untuk mengikuti perkembangan Internetworking yang terus berkembang. Kecepatan dan relevansi informasi yang sesuai dengan kebutuhan pengguna akhir menjadi fokus utama dalam komunikasi saat ini. Hal ini tercermin dalam peralihan menuju penggunaan teknologi berbasis NGN (Next Generation Network) dan era SDN (Software Defined Networking) sebagai jaringan masa depan. Komunikasi melibatkan telepon, komputer, smartpone, dan perangkat jaringan lainnya semakin sulit untuk diatur, meningkatkan risiko keamanan dan privasi bagi lembaga, perusahaan swasta, dan negara terhadap masyarakat umum. Dalam menghadapi tantangan ini, teknologi yang sedang berkembang saat ini adalah virtual private network (VPN) yang banyak digunakan sebagai solusi jaringan pribadi yang aman. Virtual private network adalah jalur komunikasi eksklusif yang dibangun melalui internet, memanfaatkan terowongan sebagai saluran komunikasi aman antara klien dan server jarak jauh yang telah disiapkan.

Keamanan siber adalah hal yang sangat penting untuk diperhatikan, walaupun terkadang beberapa organisasi memprioritaskan penampilan dan lain-lain, masalah keamanan, dan ketika sistem diretas dan sistem crash, masalah dan kerugian akan lebih besar. Kantor Dinas Kependudukan dan Pencatatan Sipil Tabalong merupakan salah satu instansi pemerintahan yang terletak di Kabupaten Tabalong, Kalimantan Selatan. Saat ini kantor dinas tersebut belum memiliki jalur koneksi internet yang cepat dan stabil untuk pengiriman data yang bersifat rahasia. Seperti yang sudah umum diketahui bahwa kantor dinas kependudukan dan pencatatan sipil mempunyai tugas melaksanakan urusan administrasi kependudukan di bidang Kependudukan dan Pencatatan Sipil berdasarkan Azas Otonomi dan Tugas Pembantuan.

Kegiatan tersebut secara khusus terkait dengan pengiriman dan penyimpanan data kependudukan yang sangat bersifat rahasia, dan penting untuk menjaga keamanan data tersebut. Saat ini, Kantor Dinas Kependudukan dan Pencatatan Sipil Tabalong belum memiliki jalur koneksi privat untuk melindungi pengiriman data penting. Proses penyimpanan data menjadi kurang terorganisir dan terpusat, terutama selama masa pandemi ketika karyawan tidak dapat mengakses sumber daya jaringan yang sama di lokasi. Dalam konteks jaringan komputer, keamanan dalam pengiriman dan penerimaan data menjadi krusial untuk menjamin bahwa data yang dikirim tidak jatuh ke tangan pihak ketiga atau yang tidak berkepentingan, terutama jika data tersebut bersifat rahasia atau penting. Oleh karena itu, diperlukan implementasi metode-metode keamanan data pada jaringan, dan salah satu solusinya adalah dengan menggunakan Virtual Private Network (VPN) dengan metode Point to Point Tunneling Protocol (PPTP).

Metode Penelitian

A. Analisa Permasalahan

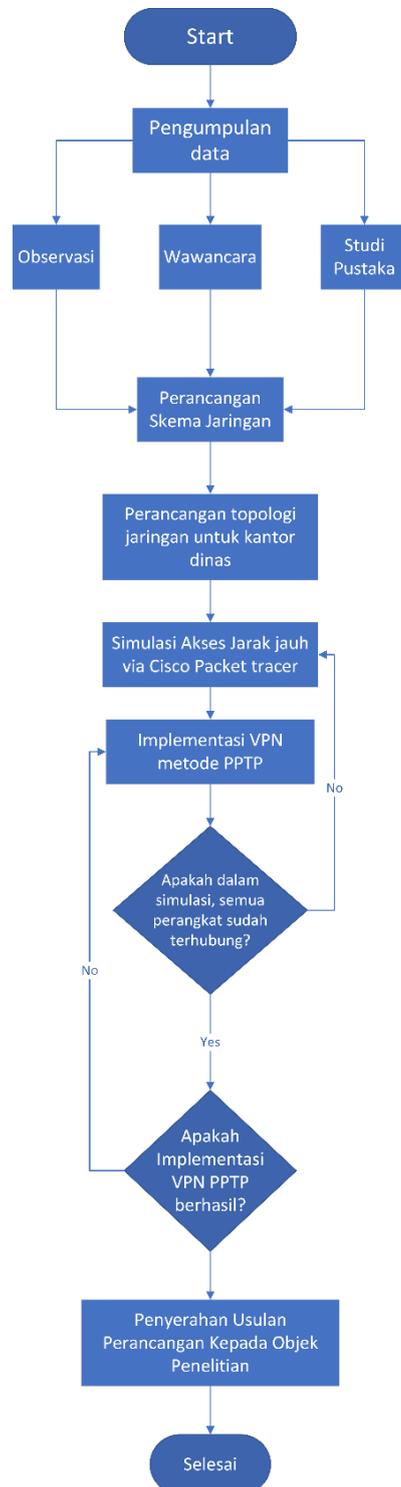
permasalahan yang akan diatasi melalui penelitian ini yaitu bagaimana membangun perancangan dan simulasi akses jarak jauh menggunakan teknologi VPN untuk kantor Dinas Kependudukan dan Pencatatan Sipil Kabupaten Tabalong).

B. Analisa Kebutuhan

1. Menghasilkan perancangan keamanan jaringan menggunakan teknologi VPN pada kantor Dinas Kependudukan dan Pencatatan Sipil Tabalong.
2. Menerapkan protokol PPTP pada perancangan keamanan jaringan yang menggunakan teknologi VPN

3. Melakukan simulasi akses jarak jauh menggunakan teknologi VPN untuk meningkatkan keamanan transfer data

C. Langkah dan Diagram Alir Penelitian



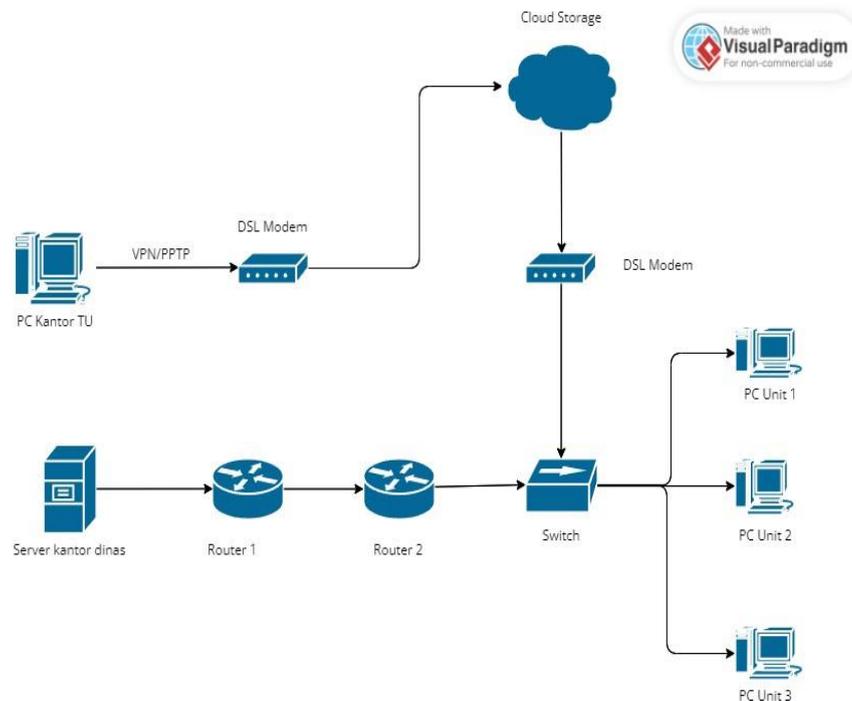
Gambar 1. Diagram Alir Penelitian

Penjelasan rinci mengenai mengenai diagram diatas adalah sebagai berikut:

- Langkah pertama pada penelitian ini adalah melakukan pengumpulan data, dimana itu memiliki 3 kegiatan sekaligus dalam satu pekan. Yang pertama adalah observasi, yaitu mengamati kantor dinas kependudukan dan pencatatan sipil tabalung, wawancara kepada tenaga IT atau Network engineering yang ada disana, dan yang terakhir studi Pustaka untuk mencari berbagai teori dan penelitian yang relevan pada penelitian ini.

- Setelah semua data sudah terkumpul, data tersebut menjadi sumber acuan dimana Langkah berikutnya adalah pembuatan perancangan skema jaringan. Langkah ini juga termasuk dalam pembuatan design dan topologi apa yang akan di gunakan.
- Setelah semua di rancang, design yang tadinya berupa gambar, mulai di implementasikan ke dalam Cisco Packet Tracer.
- Pada Cisco Packet Tracer, peneliti akan menggunakan teknologi sistem keamanan VPN dengan metode PPTP.
- Pengujian pada Cisco akan dilakukan dengan dua tahap, yang pertama adalah untuk memastikan semua perangkat terhubung dan yang kedua adalah untuk memastikan apakah VPN dapat di implementasikan dengan baik.
- Jika semua sudah tervalidasi, selanjutnya menyerahkan usulan pada kantor dinas kependudukan dan pencatatan sipil tabalong

D. Perancangan Skema Jaringan



Gambar 2. Usulan Skema Jaringan Kantor Dinas

Topologi jaringan yang diusulkan merupakan pengembangan dari topologi yang ada sebelumnya, dalam hal ini topologi yang awalnya tree setelah di konfigurasi menjadi topologi bus. Pada bagian admin terdapat garis penghubung antara admin dengan DSL modem tersebut, garis tersebut digambarkan dengan garis putus-putus untuk menekankan bahwa disana terdapat bagian implementasi VPN/PPTP digunakan. Yang mana DSL modem akan meneruskannya ke router dan switch untuk di sebarluaskan pada pengguna komputer pada kantor tersebut. Dalam mengatasi masalah keterbatasan kecepatan akses dan keamanan data di internal instansi, solusi dapat ditemukan melalui penggunaan metode PPTP (Point to Point Tunneling Protocol) pada perangkat Mikrotik yang telah terpasang di setiap gedung. PPTP adalah metode yang memungkinkan pembentukan jalur pribadi di atas jalur publik untuk meningkatkan kecepatan dan keamanan akses data.

Hasil dan Pembahasan

A.Perancangan

Bagian ini akan membahas perencanaan infrastruktur VPN, konfigurasi, dan instalasi perangkat keras serta perangkat lunak yang digunakan dalam jaringan untuk implementasi VPN. Infrastruktur yang mendukung jaringan ini terdiri dari server dan client, yang masing-masing berupa PC, hub/switch, dan perangkat lunak pendukung

1. Topologi Fisik

Topologi fisik yang menghubungkan kedua kantor ini menggunakan topologi bintang (star). Topologi star memiliki ciri utama berupa adanya konsentrator, yang bisa berupa hub, switch, atau router. Dalam penelitian ini, switch dijadikan konsentrator yang berfungsi untuk menghubungkan beberapa client dalam jaringan.

Dalam topologi fisik ini, terdapat dua tipe pengkabelan, yaitu tipe straight dan cross over. Kabel straight digunakan untuk menghubungkan switch atau hub dengan host, serta router dengan switch atau hub. Sementara itu, kabel cross over digunakan untuk menghubungkan switch dengan switch, hub dengan hub, hub dengan switch, router dengan host, dan host dengan host. Dalam penelitian ini, jenis pengkabelan yang digunakan adalah straight

2. Topologi Logika

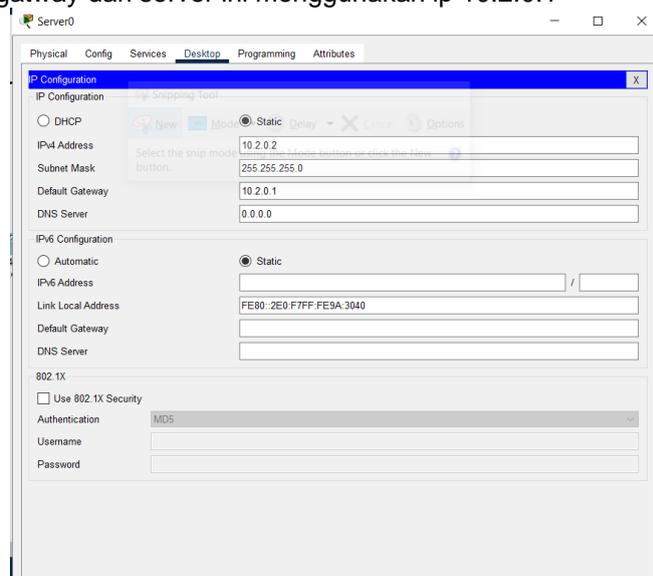
Koneksi VPN terbentuk antara kantor pusat dan kantor cabang melalui jaringan publik/internet. Alamat IP virtual pada kantor pusat adalah 10.2.0.2 dengan subnet mask 255.255.255.0. Kantor pusat terhubung ke Internet melalui ISP dengan alamat IP 10.2.0.1 dan subnet mask 255.255.255.0. Local Area Network (LAN) di kantor pusat memiliki 1 router VPN, 1 router jaringan client, 3 client PC. Kantor cabang terhubung ke Internet melalui ISP dengan alamat IP 10.2.0.1 dan subnet mask 255.255.255.0. Local Area Network (LAN) di kantor cabang memiliki network ID 10.0.0.5/24, dengan 1 PC client.

B. Perancangan

Langkah berikutnya adalah pembuatan prototipe sistem VPN, yang tujuannya adalah mensimulasikan sistem sebelum diimplementasikan pada perangkat keras yang sebenarnya. Penulis membuat simulasi ini dengan menggunakan MikroTik RouterBoard 750, dua buah laptop, dua buah modem USB, dan satu buah modem router

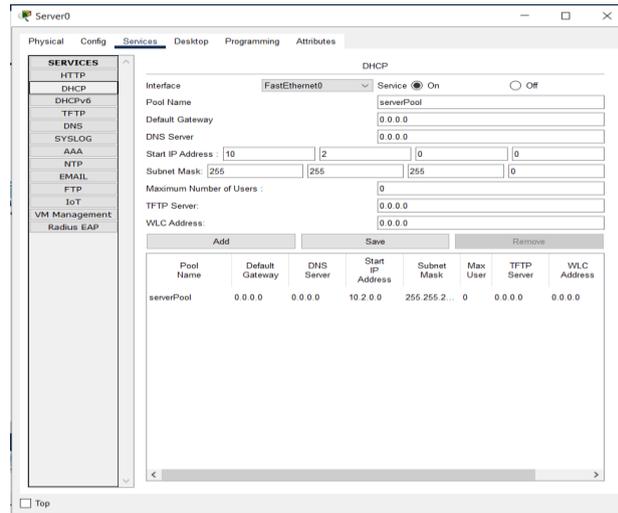
1. Konfigurasi Server

Pada tahap pertama dilakukan konfigurasi pada server dimana ditentukan berapa ip static dari server, dalam penelitian ini digunakan ip 10.2.0.2 dengan netmask 255.255.255.0 dan untuk ip jaringan atau default gateway dari server ini menggunakan ip 10.2.0.1



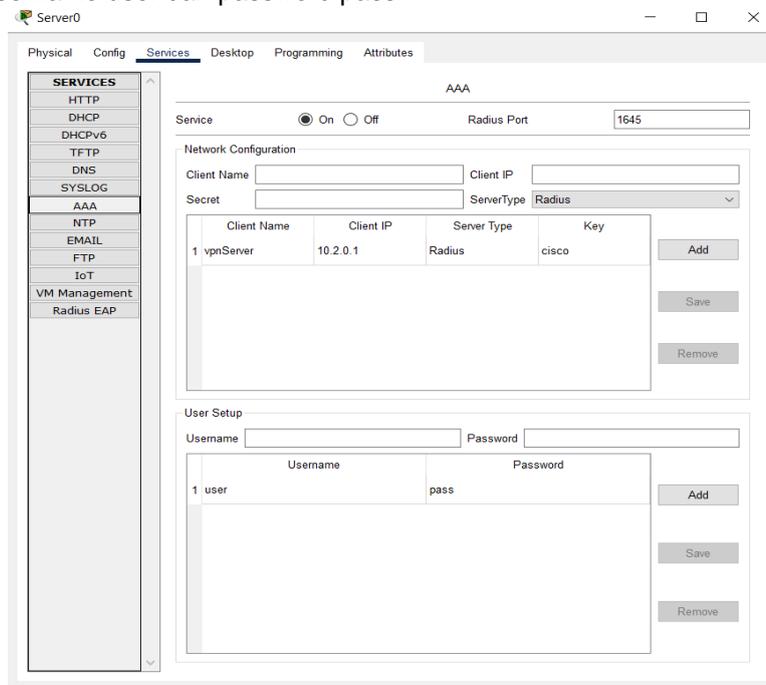
Gambar 3. Setup IP Static

Kemudian pada tab service dilakukan setting untuk DHCP dimana setting dilakukan pada koneksi fastetehernet0 dengan nama pool serverPool default gateway 0.0.0.0 DNS 0.0.0.0 dan untuk start IP menggunakan IP 10.2.0.0 dengan netmask 255.255.255.0 kemudian tekan tombol save untuk menyimpan hasil konfigurasi pada DHCP



Gambar 4. Setup IP DHCP Server

Dan selanjutnya masih di tab service dibagian AAA dilakukan penambahan untuk client AAA dengan nama client vpnServer dan IP client 10.2.0.1 dengan serial tipe Radius dan key diisi dengan cisco.terakhir dilakukan penambahan untuk user dari AAA disini user setup sebagai contoh menggunakan username user dan password pass.



Gambar 5. Setup AAA Server

2. Konfigurasi Router

Dalam setup untuk tiap router dilakukan menggunakan CLI yang tersedia pada router cisco packet tracer, untuk int fa/0 akan menggunakan ip 10.3.0.1 dan netmask 255.255.255.0 dan untuk fa1/0 menggunakan 10.2.0.1 255.255.255.0, kemudian untuk client yang berhasil login akan mendapatkan ip koneksi yang baru dimana ip dimulai dari sampai 10.1.1.100 10.1.1.200. Tujuan umum dari penggunaan dua router adalah untuk mensimulasikan koneksi antara dua jaringan yang terpisah. Dalam simulasi ini, router berperan sebagai gateway yang mengatur aliran data antara dua jaringan tersebut. Melalui konfigurasi VPN, koneksi aman dapat dibuat untuk memastikan keamanan data yang melewati jaringan. Pada skenario VPN, router berfungsi sebagai endpoint VPN dengan kemampuan untuk mengenkripsi dan mendekripsi data yang melewati koneksi. Penggunaan dua router memungkinkan simulasi pengaturan VPN site-to-site, di mana kedua ujung

jaringan terhubung melalui koneksi yang aman.dalam hal ini router satu berguna sebagai router untuk mengenkripsi jaringan dan digunakan RSA version 1 ,dan untuk router 2 berguna untuk mendekripsi jaringan

```

Router0
Physical Config CLI Attributes
IOS Command Line Interface
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Router
Router(config)#aaa new-model
Router(config)#aaa authentication login VPAUTH group radius local
Router(config)#aaa authorization network VPAUTH local
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encr aes 256
Router(config-isakmp)#authentication pre-share
^
% Invalid input detected at '^' marker.
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#crypto isakmp client configuration group ciscogroup
Router(config-isakmp-group)#key ciscogroup
Router(config-isakmp-group)#pool VPNCLIENTS
Router(config-isakmp-group)#netmask 255.255.255.0
Router(config-isakmp-group)#exit
Router(config)#crypto ipsec transform-set mytrans esp-3des esp-sha-hmac
Router(config)#crypto dynamic-map mymap 10
Router(config-crypto-map)#set transform-set mytrans
Router(config-crypto-map)#reverse-route
^
% Invalid input detected at '^' marker.
Router(config-crypto-map)#reverse-route
Router(config-crypto-map)#ex
Router(config)#crypto map mymap client authentication list VPAUTH
Router(config)#crypto map mymap isakmp authorization list VPAUTH
Router(config)#crypto map mymap client configuration address respond
Router(config)#crypto map mymap 10 ipsec-isakmp dynamic mymap
Router(config)#ip ssh version 1
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
Router(config)#spanning-tree mode pvst
Router(config)#int fa0/0
Router(config-if)#ip add 10.2.0.1
^
% Incomplete command.
Router(config-if)#ip add 10.3.0.1 255.255.255.0
Router(config-if)#duplex auto
Router(config-if)#speed auto
Router(config-if)#no sh
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Router(config-if)#ex
Router(config)#int fa0/0
    
```

Gambar 6. Konfigurasi Router 1

```

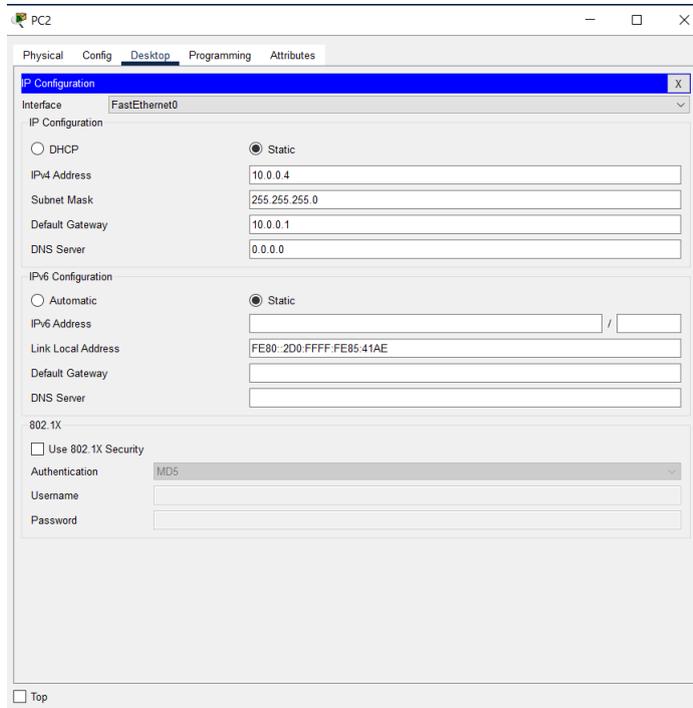
Router1
Physical Config CLI Attributes
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Router
Router(config)#ip ssh version 1
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
Router(config)#spanning-tree mode pvst
Router(config)#int fa0/0
Router(config-if)#ip add 10.3.0.2 255.255.255.0
Router(config-if)#duplex auto
Router(config-if)#speed auto
Router(config-if)#no sh
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Router(config-if)#ex
Router(config)#int fa0/1
Router(config-if)#ip add 10.0.0.1 255.255.255.0
Router(config-if)#duplex auto
Router(config-if)#speed auto
^
% Invalid input detected at '^' marker.
Router(config-if)#speed auto
Router(config-if)#sh
Router(config-if)#ex
Router(config)#class less
Router(config-cmap)#ip cef
Router(config)#ip route 10.2.0.0 255.255.255.0 10.3.0.1
Router(config)#ip route 10.1.0.0 255.255.255.0 10.3.0.1
Router(config)#ip route 10.1.1.0 255.255.255.0 10.3.0.1
Router(config)#ex
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#ping 10.3.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.0.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Router#
    
```

Gambar 7. Konfigurasi Router 2

2.Konfigurasi Tiap PC

Untuk konfigurasi PC digunakan IP static dimana untuk default gateway menggunakan ip 10.0.0.1 dan untuk PC pertama menggunakan IP static 10.0.0.2 dengan netmask 255.255.255.0, untuk PC

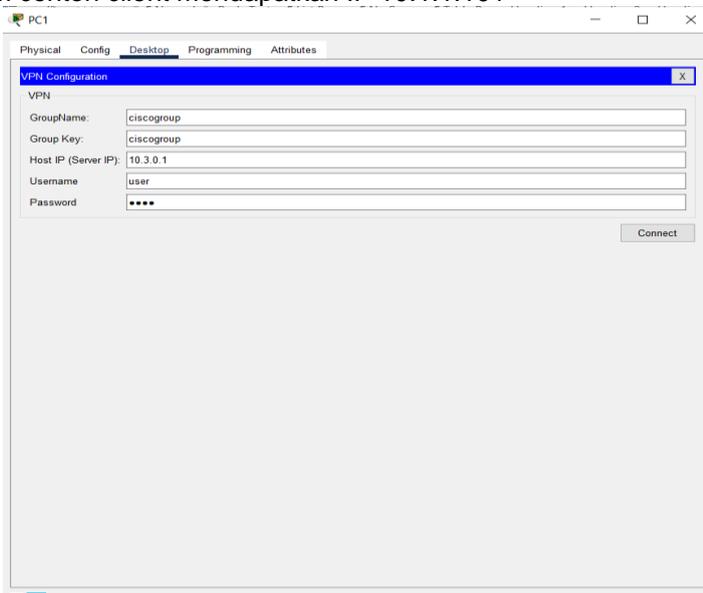
kedua menggunakan IP static 10.0.0.3 dengan netmask 255.255.255.0 dan terakhir PC tiga menggunakan IP Static 10.0.0.4 dengan netmask 255.255.255.0 dan terakhir untuk PC Client menggunakan IP 10.0.0.5 dengan netmask 255.255.255.0 yang terhubung melalui dsl modem dan Cloud



Gambar 8. Konfigurasi Tiap PC

2. Menggunakan VPN

Untuk menggunakan VPN pada cisco packet tracher ini dapat dilakukan pada tab desktop kemudian VPN,field yang diperlukan berupa group key dan group name diisikan ciscogroup dan untuk IP host nya digunakan IP 10.3.0.1 untk username user dan password nya pass kemudian connet jika berhasil connet maka akan mendapatkan IP baru dimulai IP 10.1.1.100 sampai dengan IP 10.1.1.200 dalam contoh client mendapatkan IP 10.1.1.101



Gambar 9. Form VPN

- R. Febrianti, S. Sidik, S. Susafa'ati, E. R. Nainggolan, and U. Radiah, "Implementasi VPN Berbasis Point To Point Tunneling Protocol (PPTP) Menggunakan Mikrotik Router Board," J. Infortech, vol. 3, no. 1, pp. 46–51, 2021, doi: 10.31294/infortech.v3i1.10400.
- Hermawan and M. Siddik, "Rancang Bangun Aplikasi Pembelajaran Interaktif Materi Cisco di Sekolah Tinggi Ilmu Komputer Pelita Indonesia," J. Mhs. Apl. Teknol. Komput. dan Inf., vol. 2, no. 1, pp. 62–67, 2020