

PERANCANGAN JARINGAN VPN ROUTER DENGAN METODE LINK STATE ROUTING PROTOCOLS

Timur Dali Purwanto

Teknik Komputer, Universitas Bina Darma Palembang
Jl. A. Yani No.12 Palembang
email: timoerok@gmail.com

Abstrak – Kemajuan teknologi komunikasi mempunyai pengaruh pada perkembangan pengolahan data. Untuk data yang menggunakan komputer, pengiriman data menggunakan sistem transmisi elektronik, disebut dengan istilah komunikasi data (*data communication*). Pada dasarnya jaringan LAN (*Local Area Network*) di DisHub KomInfo Pemprov SumSel mempunyai koneksi jaringan secara riil antara dua titik yang akan berhubungan antar Kominfo dan UPTD dan menerapkan jaringan komputer yang menggunakan topologi star, guna meningkatkan efisiensi dan efektifitas kerja karyawan DisHub KomInfo dan UPTD (dinas Pariwisata, Dinas Pendapatan Daerah, dan DPRD), maka perlu dibangunnya jaringan VPN (*Virtual Private Network*). Tujuan Jaringan VPN adalah menciptakan dan membentuk jaringan LAN yang tidak di batasi tempat dan waktu. Dalam perancangan jaringan VPN perlu perhatian khusus pada aspek-aspek seperti: pemilihan desain topologi jaringan, media transmisi jaringan, perangkat koneksi jaringan, serta sistem operasi jaringan yang digunakan dengan Simulasi Packet tracer. Diharapkan Penelitian ini dapat membantu proses kelancaran kerja karyawan DisHub KomInfo PemProv SumSel dan UPTD.

Kata Kunci: Jaringan LAN, Jaringan VPN, Topologi Star, Packet tracer V6.0.

I. PENDAHULUAN

Komputer adalah suatu kebutuhan alat yang amat penting untuk memudahkan manusia dalam segala bidang. Tanpa komputer manusia akan ketinggalan teknologi di dunia ini, misalnya dalam bidang pendidikan, kesehatan, pertahanan negara, dan masih banyak lagi yang membutuhkan komputer untuk membantu kita[2].

Kemajuan teknologi komunikasi mempunyai pengaruh pada perkembangan pengolahan data. Data dari satu tempat dapat dikirim ke tempat lain dengan alat telekomunikasi. Untuk data yang menggunakan komputer, pengiriman data menggunakan sistem transmisi elektronik, biasanya disebut dengan istilah komunikasi data (*data communication*). Di dalam sistem komunikasi, istilah jaringan (*network*) menurut [2] merupakan gabungan antara teknologi komputer dan teknologi telekomunikasi. Contoh jaringan yang banyak dilihat sehari-hari adalah jaringan radio dan televisi, dimana beberapa stasiun pemancar saling dihubungkan, sehingga suatu program yang sama dapat disiarkan ke segala penjuru.

IP Address digunakan sebagai alamat dalam hubungan antar *host* di internet sehingga *IP Address* menjadi sebuah sistem komunikasi yang *universal* karena merupakan metode pengalamatan yang telah diterima di seluruh dunia. Dengan menentukan *IP Address* berarti kita telah memberikan identitas yang universal bagi setiap komputer. Jika suatu komputer memiliki lebih dari satu *interface* (misalkan menggunakan dua (*ethernet*) maka kita harus memberi dua *IP Address* untuk komputer tersebut masing-masing untuk setiap *interfacenya*. Yang penting

adalah bahwa untuk berkomunikasi di *internet*, komputer harus memiliki *IP Address* yang legal. Legal dalam hal ini artinya adalah bahwa alamat tersebut dikenali oleh semua *router* di dunia dan diketahui bahwa alamat tersebut tidak ada duplikatnya di tempat lain.

Dinas Perhubungan Kominfo Provinsi Sumatra Selatan, merupakan salah satu instansi pemerintahan milik Negara. Badan instansi ini bergerak dalam bidang komunikasi dan informatika di seluruh pemrov sumsel. Pada dinas Perhubungan Kominfo ini mengelola komunikasi data antar ruang atau luar ruangan dari Kominfo ke UPTD (Unit Pelayanan Terpadu Daerah) dan telah menerapkan jaringan komputer yang menggunakan *topologi star* yang terdiri dari beberapa *workstation* pada setiap ruang yang terhubung dengan satu *switch*. Pada dasarnya jaringan LAN (*Local Area Network*) di Dinas Perhubungan Kominfo mempunyai koneksi jaringan secara riil antara dua titik yang akan berhubungan yaitu DisHub KomInfo dan UPTD. Permasalahan pada jaringan adalah belum terbangunnya koneksi yang aman dan terjamin kerahasiaannya antara DisHub Kominfo dengan UPTD melalui jaringan internet. oleh karena itu pada penelitian ini peneliti melakukan “ **Perancangan Jaringan VPN Router Dengan Metode Link State Routing Protocols**”.

II. LANDASAN TEORI

2.1. VPN (*Virtual Private Network*)

Teknologi VPN (*Virtual Private Network*) merupakan sebuah fungsi *logic* dari *switch*, yaitu

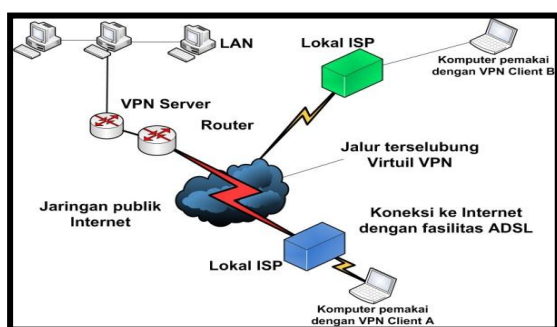
sebuah fungsi yang dikonfigurasi khusus menggunakan *software*. Sedangkan menurut [3] VPN adalah Fasilitas yang memungkinkan koneksi jarak jauh (remote access) yang aman dengan menggunakan jaringan internet untuk akses ke LAN di kantor. Fungsi ini akan membagi jaringan ke dalam beberapa jaringan *virtual* yang secara fisik masih terhubung pada *switch* yang sama. Dengan fungsi ini, jaringan komputer dapat dibuat tanpa bergantung pada lokasi fisik medianya, tetapi dapat dibuat berdasarkan kebutuhan dan fungsi yang ada. Sedangkan menurut [1] VPN merupakan suatu koneksi antar dua jaringan yang dibuat untuk mengkoneksikan kantor pusat, kantor cabang, *telecommuters*, *suppliers*, dan rekan bisnis lainnya, ke dalam suatu jaringan dengan menggunakan infrastruktur telekomunikasi umum dan menggunakan metode enkripsi tertentu sebagai media Pengamanannya

VPN adalah sebuah koneksi private melalui jaringan publik (internet). Disini ada dua kata yang penting yaitu:

- Virtual network*, yang berarti jaringan yang terjadi hanya bersifat *virtual*. Tidak ada koneksi jaringan secara riil antara dua titik yang akan berhubungan.
- Private*, jaringan yang terbentuk *bersifat private* dimana tidak semua orang bisa mengaksesnya. Data yang dikirimkan *terenkripsi* sehingga tetap rahasia meskipun melalui jaringan publik.

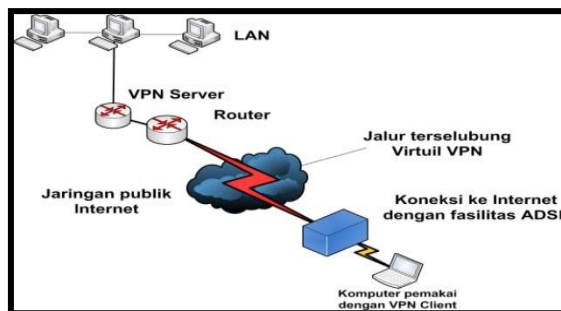
Menurut IETF, Internet Engineering Task Force, VPN is an emulation of private Wide Area Network (WAN) using shared or public IP facilities, such as the Internet or private IP backbones. (VPN merupakan suatu bentuk private internet yang melalui public network (internet), dengan menekankan pada keamanan data dan akses global melalui internet. Hubungan ini dibangun melalui suatu *tunnel* (terowongan) *virtual* antara 2 *node*).

Konsep kerja VPN pada dasarnya VPN Membutuhkan sebuah *server* yang berfungsi sebagai penghubung antar PC. Dapat digambarkan sebagai berikut :



Gambar 1. VPN Server dan VPN Client

Untuk menghubungkan dua komputer secara *private* dengan jaringan internet maka dapat digambarkan seperti ini:



Gambar 2. Site to Site VPN

Jadi semua koneksi diatur oleh VPN Server sehingga dibutuhkan kemampuan VPN Server yang memadai agar koneksinya bisa lancar.

2.1.1. Cara Kerja Jaringan VPN

Adapun cara kerja VPN sebagai berikut :

- VPN membutuhkan sebuah server yang berfungsi sebagai penghubung antar PC, *Server VPN* ini bisa berupa komputer dengan aplikasi *VPN Server* atau sebuah *Router*
- Untuk memulai sebuah koneksi, komputer dengan aplikasi *VPN Client* mengontak *serverVPN*, *VPN server* kemudian *memverifikasi username* dan *password*. Dan apabila berhasil maka *VPN server* memberikan *IP Address* baru pada komputer client dan selanjutnya sebuah koneksi / *tunnel* akan terbentuk.
- Selanjutnya komputer *client* bisa digunakan untuk mengakses berbagai *resource* (komputer atau LAN) yang berada dibelakang *VPN server* misalnya melakukan transfer data, ngeprint dokumen, *browsing* dengan *gateway* yang diberikan dari *VPN Server*, melakukan *remote desktop* dan lain sebagainya[3].

2.1.2. Manfaat Jaringan VPN

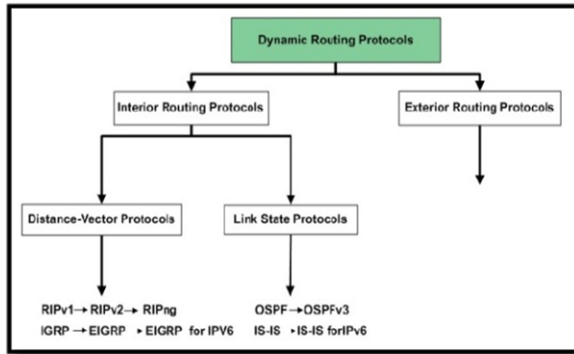
Manfaat Jaringan VPN adalah sebagai berikut:

- Remote Access*, dengan VPN kita dapat mengakses komputer atau jaringan kantor, dari mana saja selama terhubung ke internet
- Keamanan, dengan koneksi VPN kita bisa berselancar dengan aman ketika menggunakan akses *internet publik* seperti *hotspot* atau *internet cafe*.
- Menghemat biaya *setup* jaringan, VPN dapat digunakan sebagai *teknologi alternatif* untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif kecil, karena transmisi data teknologi VPN menggunakan media *jaringan public* yang sudah ada tanpa perlu membangun jaringan pribadi [3].

2.2. Klasifikasi Protokol Dynamic Routing

Menurut [5] pada protokol *routing* kelas *Interior Gateway Protocols (IGPs) dynamic routing* diklasifikasi menjadi dua, yaitu *distance vector routing* dan *link-state routing*. Untuk klasifikasi *dynamic routing protocol* secara keseluruhan terlihat

seperti pada Gambar 1. Pembagian pada *dynamic routing protocol* dibedakan berdasarkan karakteristik dan cara kerjanya masing-masing



Gambar 3. Klasifikasi *Dynamic Routing Protocol*

2.3. Packet Tracer

Packet tracer adalah sebuah *simulator protocol* jaringan yang dikembangkan oleh Cisco System. *Paket Tracer* dapat mensimulasikan berbagai macam *protocol* yg digunakan pada jaringan baik secara *realtime* maupun dengan *mode simulasi*.

Packet tracer merupakan sebuah *software* simulasi jaringan yang digunakan untuk pembelajaran jaringan komputer pada umumnya dan *trouble shooting* jaringan pada pembelajaran CCNA pada khususnya. *Packet tracer* menyediakan fasilitas untuk membuat *simulasi*, *visualisasi* dan *animasi* dalam pembuatan dan *trouble shooting* jaringan komputer. *Software* ini sangat bermanfaat untuk membuat suatu usulan rancangan jaringan komputer dan menampilkannya dalam bentuk simulasi sebelum usulan sebuah jaringan komputer diterapkan dalam dunia nyata. Sebagai *software* simulasi tentu saja terdapat kekurangan didalamnya, salah satunya adalah keterbatasan peralatan yang disediakan dan keterbatasan fungsi perintah yang dapat dijalankan. (<http://www.ee.ui.ac.id/netla> & Modul Praktikum Jaringan Komputer Universitas Indonesia)^[4]

Salah satu aspek yang paling berharga dari *packet tracer* adalah kemampuan untuk menjalankan simulasi setelah membangun / *mendesain* jaringan. *User* dapat membuat sebuah jaringan dan membuat beberapa jaringan yang berbeda *skenario*nya dalam pengiriman paket dari sumber yang berbeda ke tujuan yang berbeda pula. *User*-pun dapat menyimpan serta membuka *file* yang telah dibuatnya itu.

Network devices yang dapat didukung oleh *packet tracer* antara lain :

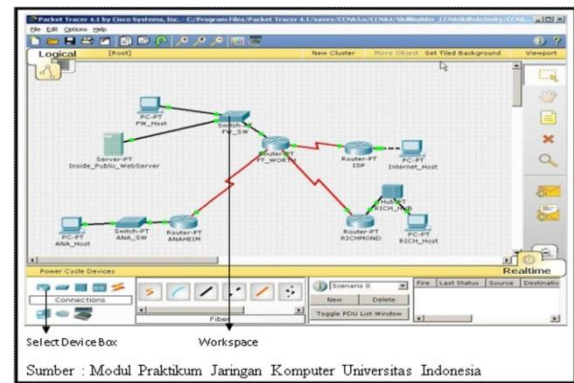
- a. Router
- b. Cloud
- c. Switch
- d. Bridge
- e. Repeater
- f. Hub
- g. Wireless
- h. Access Point
- i. PC
- j. Server

Interfaces yang dapat didukung oleh *packet tracer* antara lain:

- a. Ethernet (copper)
- b. Fast Ethernet (copper and fiber)
- c. Gigabit Ethernet (copper and fiber)
- d. Serial
- e. Modem
- f. Wireless

Bandwidth yang dapat didukung oleh *packet tracer* yaitu :

- a. 56 Kbps
- b. 128 Kbps
- c. 384 Kbps
- d. 786 Kbps
- e. 1.544 Mbps
- f. 2.048 Mbps

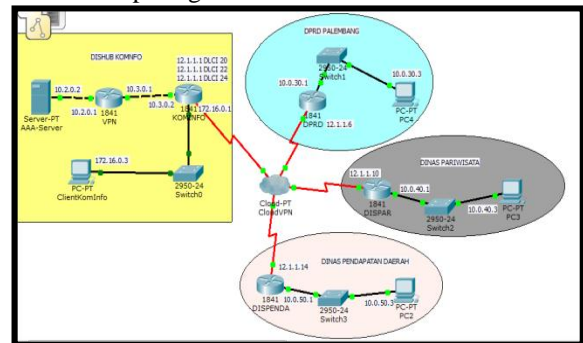


Gambar 4. *Interface Packet Tracer*

III. PEMBAHASAN

3.1. Hasil Perancangan Topologi Jaringan VPN

KomInfo Provinsi SumSel yang terletak di Jln. Kapten Rivai ingin menghubungkan UPTD (DPRD, DISPAR,dan DISPENDA). Untuk itu mereka ingin membangun koneksi yang aman dan terjamin kerahasiaannya antara kantor Dishub Kominfo dengan UPTD tersebut di kota Palembang melalui *public network*. Seperti gambar dibawah ini :



Gambar 5. Hasil Perancangan *Topologi VPN* DisHub KomInfo Provinsi SumSel ke UPTD

Berdasarkan gambar diatas dapat dilihat bahwa jaringan DisHub KomInfo Provinsi SumSel di Jln. Kapten Rivai Palembang ditambahkan satu buah VPN Server, satu buah *router vpn*, satu buah *router* KomInfo dan satu buah *switch* pada setiap kantoryang nantinya akan bertindak untuk merespon permintaan

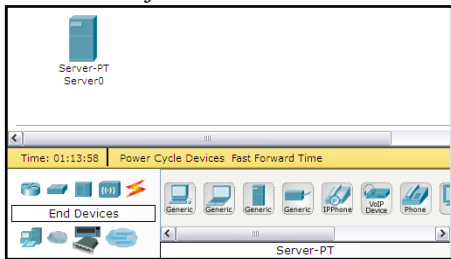
VPN dan melakukan autentikasi dari *mobile user* ataupun kantor UPTD yang ingin mengakses VPN di DisHub KomInfo Provinsi SumSel.

3.2. Hasil konfigurasi Routing VPN menggunakan metode Link State

1. Konfigurasi Server AAA (Authentication, Authorization, Accounting)

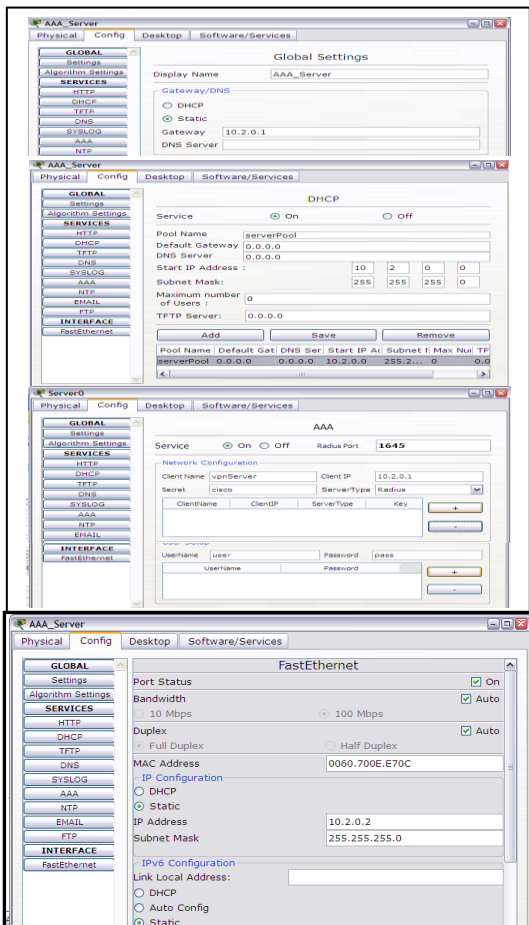
Server AAA digunakan untuk mengenali pengguna yang memasuki system dan memberikan wewenang bagi pengguna untuk mengakses resource pada system berdasarkan hak yang telah diberikan.

a. Aktifkan Server-PT dengan cara drag ke media kerja



Gambar 6. mengaktifkan Server-PT

b. Double click untuk membuka menu setting Server-PT dan setting sesuai tahapan gambar berikut



Gambar 7. Konfigurasi Server AAA

2. Konfigurasi Router VPN

Pada konfigurasi *Router VPN* dikantor DisHub KomInfo untuk memberi konekfitas bagi jaringan UPTD untuk dapat terkoneksi dalam server radius berdasarkan wewenang yang telah diberikan server. Dapat dilihat konfigurasi dibawah ini :

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#hostname routerVPN
routerVPN(config)#aaa new-model
routerVPN(config)#aaa authentication login
VPNAUTH group radius local
routerVPN(config)#aaa authorization network
VPNAUTH local
routerVPN(config-isakmp-group)#pool VPNCLIENTS
routerVPN(config-isakmp-group)#netmask
255.255.255.0
routerVPN(config-isakmp-group)#crypto ipsec
transform-set mytrans esp-3des esp-sha-hmac
routerVPN(config)#crypto dynamic-map mymap 10
routerVPN(config-crypto-map)#set transform-set
mytrans
routerVPN(config-crypto-map)#reverse-route
routerVPN(config-crypto-map)#crypto map mymap
client authentication list VPNAUTH
routerVPN(config)#crypto map mymap isakmp
authorization list VPNAUTH
routerVPN(config)#crypto map mymap client
configuration address respond
routerVPN(config)#crypto map mymap 10 ipsec-
isakmp dynamic mymap
routerVPN(config)#ip ssh version 1
Please create RSA keys (of at least 768 bits size) to
enable SSH v2.
routerVPN(config)#spanning-tree mode pvst
routerVPN(config)#interface FastEthernet0/0
routerVPN(config-if)#ip address 10.3.0.1
255.255.255.0
routerVPN(config-if)#duplex auto
routerVPN(config-if)#speed auto
routerVPN(config-if)#crypto map mymap
*Jan 3 07:16:26.785: %CRYPTO-6-
ISAKMP_ON_OFF: ISAKMP is ON
routerVPN(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0,
changed state to up
routerVPN(config-if)#interface FastEthernet0/1
routerVPN(config-if)#ip address 10.2.0.1
255.255.255.0
routerVPN(config-if)#duplex auto
routerVPN(config-if)#speed auto
routerVPN(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/1,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/1, changed state to up
    
```

```

routerVPN(config-if)#interface Vlan1
routerVPN(config-if)#no ip address
routerVPN(config-if)#shutdown
routerVPN(config-if)#ip local pool
VPNCLIENTS 10.1.1.100 10.1.1.200
routerVPN(config)#ip route 10.0.0.0
255.255.255.0 10.3.0.2
routerVPN(config)#ip route 10.0.0.0
255.255.255.0 10.3.0.2
routerVPN(config)#ip route 172.16.0.0
255.255.255.0 10.3.0.2
routerVPN(config)#ip route 10.0.40.0
255.255.255.0 10.3.0.2
routerVPN(config)#ip route 10.0.30.0
255.255.255.0 10.3.0.2
routerVPN(config)#ip route 10.0.50.0
255.255.255.0 10.3.0.2
routerVPN(config)#radius-server host 10.2.0.2
auth-port 1645 key cisco
routerVPN(config)#exit
routerVPN#
%SYS-5-CONFIG_I: Configured from console by
console

```

3. Konfigurasi Jaringan Router VPN

Pada konfigurasi *Router* KomInfo (R1) dikantor DisHub KomInfo untuk memberi Konekfitas bagi jaringan UPTD dan kominfo menggunakan metode link state routing protocols. Menurut Muhammad S (2010)[5] OSPF adalah *routing protocol* yang menggunakan konsep *area*. Kelebihan dari OSPF dibandingkan dengan RIP adalah kecepatan dalam melakukan konvergensi dan lebih luasnya jaringan yang bisa dijangkau, dapat dilihat konfigurasi dibawah ini:

```

Router>en
R1#conf t
Enter configuration commands, one per line. End
with CNTL/Z.
Router(config)#hostname routerVPN
R1(config)#ip ssh version 1
Please create RSA keys (of at least 768 bits size) to
enable SSH v2.
R1(config)#spanning-tree mode pvst
R1(config)#interface FastEthernet0/1
R1(config-if)#ip address 10.3.0.2 255.255.255.0
R1(config-if)#duplex auto
R1(config-if)#speed auto
R1(config-if)#no shutdown
R1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/1, changed state to up
R1(config-if)#interface FastEthernet0/0
R1(config-if)#ip address 172.16.0.1 255.255.255.0
R1(config-if)#duplex auto
R1(config-if)#speed auto
R1(config-if)#no shutdown
R1(config-if)#interface Vlan1
R1(config-if)#no ip address
R1(config-if)#shutdown
R1(config-if)#int s0/1/0
R1(config-if)#encapsulation frame-relay

```

```

R1(config-if)#no sh
R1(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial0/1/0, changed state to up
R1(config-if)#ex
R1(config)#int s0/1/0.20 point-to-point
R1(config-subif)#
%LINK-5-CHANGED: Interface Serial0/1/0.20, changed state
to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/1/0.20, changed state to up
R1(config-subif)#ip address 12.1.1.5 255.255.255.252
R1(config-subif)#frame-relay interface-dlci 20
R1(config-subif)#ip ospf network broadcast
R1(config-subif)#no sh
R1(config-subif)#ex
R1(config)#int s0/1/0.22 point-to-point
R1(config-subif)#
%LINK-5-CHANGED: Interface Serial0/1/0.22, changed state
to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/1/0.22, changed state to up
R1(config-subif)#ip address 12.1.1.9 255.255.255.252
R1(config-subif)#frame-relay interface-dlci 22
R1(config-subif)#ip ospf network broadcast
R1(config-subif)#no sh
R1(config-subif)#exit
R1(config)#int s0/1/0.24 point-to-point
R1(config-subif)#
%LINK-5-CHANGED: Interface Serial0/1/0.24, changed state
to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/1/0.24, changed state to up
R1(config-subif)#ip address 12.1.1.13 255.255.255.252
R1(config-subif)#frame-relay interface-dlci 24
R1(config-subif)#ip ospf network broadcast
R1(config)#router ospf 1
R1(config-router)#network 10.0.0.0 0.0.0.255 area 0
R1(config-router)#network 10.1.0.0 0.0.0.255 area 0
R1(config-router)#network 10.1.1.0 0.0.0.255 area 0
R1(config-router)#network 10.3.0.0 0.0.0.255 area 0
R1(config-router)#network 10.2.0.0 0.0.0.255 area 0
R1(config-router)#network 12.1.1.4 0.0.0.3 area 0
R1(config-router)#network 12.1.1.8 0.0.0.3 area 0
R1(config-router)#network 12.1.1.12 0.0.0.3 area 0
R1(config-router)#network 12.1.1.16 0.0.0.3 area 0
R1(config-router)#network 172.16.0.0 0.0.0.255 area 0
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

```

Dari hasil penelitian yang penulis lakukan dengan judul “**Perancangan Jaringan VPN Router Dengan Metode Link State Routing Protocols**”, penulis mengambil kesimpulan :

1. Penerapan teknologi jaringan VPN akan meningkatkan kualitas pelayanan yang dihasilkan jaringan tersebut kepada semua pihak yang terlibat didalamnya dan dapat meningkatkan *performance* jaringan kantor DisHub KomInfo dan UPTD Palembang dibandingkan dengan jaringan yang terdahulu.
2. Penggunaan teknologi VPN menjadi solusi agar *client* (dalam hal ini *Solution Engineer*) dapat terkoneksi ke PC *Server*.
3. Selain itu penggunaan VPN memberikan kelebihan dalam hal keamanan jaringan karena memiliki kelebihan yaitu *User Authentication*, *Address*

Management, Data Encryption, Key Management, dan Multiprotocol Support .

DAFTAR REFERENSI

- [1] *Archer Kevin, dkk, 2001, "Voice and Data Security", Sams Publishing., USA., 14-15 pp.*
- [2] *Dede Sopandi.2010."Instalasi Dan Konfigurasi Jaringan Komputer". Bandung. Informatika.*
- [3] *Hendra Wijaya. 2011. "belajar sendiri Cisco DSL Router. ASA Firewall dan VPN". Jakarta. PT Elex Media Komputindo.*
- [4] *Universitas Srwijaya. 2011."Modul Jaringan Komputer".Palembang.*
- [5] *Syafrudin Muhammad. 2010. "Analisa Unjuk Kerja Routing Protocol RIPng dan OSPFv3 Pada*

Jaringan IPv6". Skripsi. Fakultas Teknik Departemen Teknik Elektro Universitas Indonesia. Depok.

Biodata Penulis

Timur Dali Purwanto, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Teknik Informasi Universitas Bina Darma Palembang, lulus tahun 2010. Memperoleh gelar Magister Komputer (M.Kom) Program Pasca Sarjana Magister Ilmu Komputer Universitas Bina DarmaPalembang, lulus tahun 2011. Saat ini menjadi Dosen di Universitas Bina Darma Palembang.