IMPLEMENTASI DAN ANALISA L2TP/IPSEC MENGGUNAKAN ROUTER CISCO SERI 2900

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Teknik
Pada Fakultas Teknik
Universitas Islam Riau Pekanbaru

OLEH :

M.Nawawi Ridho Maja
143510118

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS ISLAM RIAU
PEKANBARU
2019

LEMBAR PENGESAHAN PEMBIMBING SKRIPSI

Nama : M Nawawi Ridho Maja

NPM : 143510118

Jurusan : Teknik

Program Studi : Teknik Informatika

Jenjang Pendidikan : Strata Satu (S1)

Judul Skripsi : Implementasi Dan Analisa L2tp/Ipsec Menggunakan Router Cisco Sebagai Server

Format sistematika dan pembahasan materi pada masing-masing bab dan sub bab dalam skripsi ini telah dipelajari dan dinilai relatif telah memenuhi ketentuan-ketentuan dan kriteria - kriteria dalam metode penulisan ilmiah. Oleh karena itu, skripsi ini dinilai layak dapat disetujui untuk disidangkan dalam ujian komprehensif.

Pekanbaru, 18 Desember 2019

Disetujui Oleh

Dosen Pembimbing

APRI SISWANTO, S.Kom., M.Kom

Disahkan Oleh :

Dekan Fakultas Teknik

Ir. H. ABDUL AZIS DUS ZAINI, MT., MS., TR

NPK : 88 03 02 098

Ketua Prodi Teknik Informatika

AUSE LABELLAPANSA, ST., M.Cs., M.Kom

LEMBAR PENGESAHAN
TIM PENGUJI UJIAN SKRIPSI

Nama	:	M Nawawi Ridho Maja
NPM	:	143510118
Jurusan	:	Teknik
Program Studi	:	Teknik Informatika
Jenjang Pendidikan	:	Strata Satu (S1)
Judul Skripsi	:	Implementasi Dan Analisa L2tp/Ipsec Menggunakan Router Cisco Seri 2900

Skripsi ini secara keseluruhan dinilai telah memenuhi ketentuan-ketentuan dan kaidah-kaidah dalam penulisan penelitian ilmiah serta telah diuji dan dapat dipertahankan dihadapan tim penguji. Oleh karena itu, Tim Penguji Ujian Skripsi Fakultas Teknik Universitas Islam Riau menyatakan bahwa mahasiswa yang bersangkutan dinyatakan **Telah Lulus Mengikuti Ujian Komprehensif Pada Tanggal 13 Desember 2019** dan disetujui serta diterima untuk memenuhi salah satu syarat guna memperoleh gelar Sarjana Strata Satu Bidang Ilmu **Teknik Informatika.**

Pekanbaru, 13 Desember 2019

Tim Penguji

1. Dr. Evizal., ST., M.Eng	Sebagai Tim Penguji I	(.....)
2. Abdul Syukur, S.Kom., M.Kom	Sebagai Tim Penguji II	(.....)

Disetujui Oleh

Dosen Pembimbing

APRI SISWANTO, S.Kom., M.Kom

Disahkan Oleh :

Dekan Fakultas Teknik	Ketua Prodi Teknik Informatika
Dr. H. ABD. KADIR ZAINI, MT.,MS., TR	AUSE LABELLAPANSA, ST., M.Cs., M.Kom
NIK : 88 03 02 098	

LEMBAR PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan dibawah ini :

Nama : M Nawawi Ridho Maja

Tempat, Tgl Lahir : Semukut, 10 April 1996

Alamat : Jalan Karya 1 - Pekanbaru

Adalah Mahasiswa Universitas Islam Riau yang terdaftar pada :

Fakultas : Teknik

Program Studi : Teknik Informatika

Jenjang Pendidikan : Strata-1 (S1)

Dengan ini menyatakan dengan sesungguhnya bahwa skripsi yang saya tulis adalah benar dan asli hasil dari penelitian yang telah saya lakukan dengan judul **"Implementasi Dan Analisa L2TP/IPSEC Menggunakan Router Cisco Seri 2900".**

Apabila dikemudian hari ada yang merasa dirugikan dan atau menuntut karena penelitian ini menggunakan sebagian hasil tulisan atau karya orang lain tanpa mencantumkan nama penulis yang bersangkutan, atau terbukti karyai lmiah ini **bukan** karya saya sendiri atau **plagiat** hasil karya orang lain, maka saya bersedia menerima sanksi sesuai dengan peraturan perundang-undangan yang berlaku.

Demikian surat pernyataan ini saya buat dengan sesungguhnya untuk dapat digunakan sebagaimana mestinya.

Pekanbaru, 16 Desember 2019

Yang membuat pernyataan,

M Nawawi Ridho Maja

LEMBAR IDENTITAS PENULIS

NPM	: 143510118
Nama Lengkap	: M Nawawi Ridho Maja
Tempat, Tgl Lahir	: Semukut, 10 April 1996
Alamat	: Jalan Karya 1
Nama Ayah	: Mahmud
Nama Ibu	: Nuraini
Nomor Handphone	: 082387822744
Fakultas	: Teknik
Program Studi	: Teknik Informatika
Judul Skripsi	: Implementasi Dan Analisa L2TP/IPSEC Menggunakan Router Cisco Seri 2900
Tahun Masuk	: 2014
Tahun Lulus	: 2019

Pekanbaru, 16 Desember 2019

M Nawawi Ridho Maja
143510118

DAFTAR RIWAYAT HIDUP

1. Data Personal

NPM	: 143510118
Nama Lengkap	: M Nawawi Ridho Maja
Tempat, Tgl.Lahir	: Semukut, 10 April 1996
Jenis Kelamin	: Perempuan
Agama	: Islam
Jenjang	: Strata 1 (S1)
Program Studi	: Teknik Informatika
Alamat	: Jalan Karya 1
Nomor Handphone	: 082387822744
Email	: ridhomaja1996@student.uir.ac.id

2. Pendidikan

No	Jenjang	Nama Lembaga	Tahun
1	SD	SDN 22 Semukut	2002 - 2008
2	MTS	MTSN Semukut	2008 - 2011
3	SMK	SMKN 1 Selat Panjang	2011 - 2014
4	PT	Universitas Islam Riau	2014 - 2019

Demikian daftar riwayat hidup ini dibuat dengan sebenarnya.

Pekanbaru, 16 Desember 2019
Mahasiswa Ybs,

M Nawawi Ridho Maja

HALAMAN PERSEMBAHAN

Assalamualaikum warahmatullahi wabarakatuh.

Puji syukur kehadirat Allah SWT yang Maha Pengasih lagi Maha Panyayang atas rahmat, hidayah, dan inayah-Nya, sehingga penulis dapat menyelesaikan laporan skripsi yang berjudul "Implementasi Dan Analisa L2TP/IPSEC Menggunakan Router Cisco Seri 2900" ini tepat pada waktunya.Laporan skripsi ini disusun untuk memenuhi salah satu syarat untuk memperoleh gelar sarjana pada Fakultas Teknik Universitas Islam Riau.

Dalam penyusunan laporan skripsi ini, penulis sadar bahwa tanpa bantuan dan bimbingan dari berbagai pihak maka laporan skripsi ini sulit untuk terwujud. Untuk itu dalam kesempatan ini penulis ingin menyampaikan ucapan terima kasih kepada:

1. Yang teristimewa Bapak Mahmud dan Ibuku Nuraini yang tidak pernah lelah berkorban, memberi segala dukungan, dan selalu mendoakan anaknya agar menjadi orang yang berguna dan sukses dalam mewujudkan cita-cita
2. Abangku tersayang M Idola Mursyid Maja yang selalu memberikan motivasi dan mendoakan penulis dalam menyelesaikan skripsi ini
3. Bapak Apri Siswanto, S.Kom., M.Kom selaku pembimbing yang telah dengan sabar dan ikhlas membimbing, membantu, dan memberikan arahan dalam menyelesaikan laporan skripsi ini dengan baik

4. Bapak dan Ibu Dosen Teknik Informatika Universitas Islam Riau yang telah memberikan ilmu yang bermanfaat selama masa perkuliahan
5. Sahabat sahabat tersayangku Romy Saputra, Bayu Purnomo aji, M Subahagia Adonnoto, Putra Kurniawan, Rozy Sunaryo, Zalian Hasrin, Ilham Saputra, Novia Riska Arsela, Elsa Lutfy Maghfiroh dan sahabat sahabatku yang lain yang tidak dapat disebutkan satu persatu, yang telah meluangkan waktunya untuk membantu dan memberikan semangat, nasihat serta motivasi dalam menyelesaikan skripsi ini. Terima kasih atas segala dukungannya, semoga Allah SWT membalasnya dengan kebaikan kebaikan, Aamiin.
6. Teman teman Kelas A dan B serta Konsentrasi Jaringan Komputer Angkatan 2014. Terima kasih atas kebersamaan yang telah dilewati.

Akhir kata penulis mohon maaf atas kekeliruan dan kesalahan yang terdapat dalam skripsi ini dan berharap semoga skripsi ini dapat memberikan manfaat bagi pembaca.

Pekanbaru,16 Desember 2019

M Nawawi Ridho Maja
143510118

KATA PENGANTAR

بسم الله الرحمن الرحيم

Puji syukur kehadirat Allah SWT yang Maha Pengasih lagi Maha Panyayang atas rahmat, hidayah, dan inayah-Nya, sehingga penulis dapat menyelesaikan laporan skripsi yang berjudul "Implementasi Dan Analisa L2TP/IPSEC Menggunakan Router Cisco Seri 2900" ini tepat pada waktunya. Laporan skripsi ini disusun untuk memenuhi salah satu syarat untuk memperoleh gelar sarjana pada Fakultas Teknik Universitas Islam Riau.

Dalam penyusunan laporan skripsi ini, penulis sadar bahwa tanpa bantuan dan bimbingan dari berbagai pihak maka laporan skripsi ini sulit untuk terwujud. Untuk itu dalam kesempatan ini penulis ingin menyampaikan ucapan terima kasih kepada:

1. Bapak Ir. H. Abd Kudus Zaini, MT selaku dekan Fakultas Teknik Universitas Islam Riau
2. Ibu Dr. Kurnia Hastuti, ST., MT selaku Wakil Dekan I, Bapak M. Ariyon, ST., MT selaku Wakil Dekan II, dan Bapak Ir. Syawaldi, M.Sc selaku Wakil Dekan III Fakultas Teknik Universitas Islam Riau
3. Ibu Ause Labellapansa, ST., M.Cs., M.Kom, selaku Kepala Prodi Teknik Informatika
4. Bapak Apri Siswanto, S.Kom., M.Kom selaku pembimbing, yang telah membantu dan memberikan pengarahan serta bimbingan dalam menyelesaikan laporan skripsi ini dengan baik

5. Seluruh Dosen Teknik Informatika beserta staff tata usaha
6. Semua pihak yang telah membantu dalam penyelesaian laporan skripsi ini

Penulis menyadari bahwa laporan skripsi ini masih jauh dari kesempurnaan baik dalam bentuk penyusunan maupun materinya. Kritik konstruktif dari pembaca sangat penulis harapkan demi kesempurnaan laporan ini. Akhir kata semoga laporan skripsi ini dapat memberikan manfaat bagi sekalian.

Pekanbaru, 20 Mei 2019

Penulis

M Nawawi Ridho Maja

Implementasi Dan Analisa L2TP/IPSEC Menggunakan Router Cisco Seri 2900

M Nawawi Ridho Maja
Fakultas Teknik
Program Studi Teknik Informatika
Universitas Islam Riau
Email : ridhomaja1996@student.uir.ac.id

ABSTRAK

Perkembangan teknologi yang pesat khususnya internet membuatnya dapat diakses bebas di mana saja dan dapat menggunakan apa saja, seperti laptop, tablet, dan handphone. Perkembangan pesat dapat berdampak baik, seperti kecepatan dalam memperoleh informasi dan juga dapat berdampak buruk pada masalah keamanan, misalnya pencurian data. Metode yang digunakan untuk mengatasi agar tidak terjadinya masalah keamanan data seperti pencurian data adalah dengan menggunakan VPN (Virtual Private Network), VPN mempunyai beberapa macam protocol yaitu Point To Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Internet Protocol Security (IPSEC) dan Secure Socket Layer (SSL) yang semuanya mempunyai kelebihan dan kekurangannya masing masing, Protocol yang digunakan adalah L2TP/IPSEC. Dengan menggunakan protocol L2TP/IPSec ini maka data yang dikirim ataupun diterima dalam kondisi aman dan sudah dienkripsi dengan baik dan akan dikirim melalui sebuah tunnel. Sehingga pihak-pihak yang tidak berhak untuk mengakses tidak bisa melihat dan mengakses data tersebut. Karena L2TP/IPSec memberikan atau menyediakan layanan keamanan yang sangat baik diantara layanannya yaitu data integrity, confidentiality, authentication, dan anti replay.

Kata kunci: Keamanan, Protokol, Tunnel.

Implementing and Analyzing L2tp / IPSec Using Cisco 2900 Series Router

M Nawawi Ridho Maja
Faculty of Engineering
Informatics Engineering
Islamic University of Riau
Email: ridhomaja1996@student.uir.ac.id

ABSTRACT

The rapid development of technology, especially the internet makes it freely accessible anywhere and can use anything, such as laptops, tablets, and mobile phones. Rapid development can have a good effect, such as speed in obtaining information and can also have a negative impact on security issues, such as data theft. The method used to overcome the avoidance of data security problems such as data theft is to use VPN (Virtual Private Network), VPN has several protocols, namely Point To Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Internet Protocol Security (IPSEC) and Secure Socket Layer (SSL) all of which have their own advantages and disadvantages. The protocol used is L2TP / IPSEC. By using this L2TP / IPSec protocol, the data sent or received is safe and has been encrypted properly and will be sent through a tunnel. So parties who are not entitled to access cannot see and access the data. Because L2TP / IPSec provides or provides excellent security services among services, namely data integrity, confidentiality, authentication, and anti-replay.
***Keywords**: Security, Protocol, Tunnel.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang pesat khususnya internet membuatnya dapat diakses bebas di mana saja dan dapat menggunakan apa saja, seperti laptop, tablet, dan handphone. Perkembangan pesat dapat berdampak baik, seperti kecepatan dalam memperoleh informasi dan juga dapat berdampak buruk pada masalah keamanan, misalnya pencurian data.

Ada beberapa macam metode untuk mengatasi permasalahan keamanan data didalam suatu jaringan, contohnya dengan mengenkripsi data, tanda tangan digital (*digital signature*), maupun memasang *firewall*. Beberapa solusi tersebut bisa meningkatkan keamanan data disebuah jaringan, namun juga mempunyai kelemahan, seperti *firewall* dapat mencegah penyusup dari luar, tetapi tidak dapat mencegah jika data disadap oleh orang yang ada didalam jaringan itu sendiri. Begitu pula dengan mengenkripsi data ataupun *digital signature*, dalam hal ini sangat dibutuhkan kesadaran dari pihak pengirim data untuk melakukan enkripsi yang kadang sangat merepotkan dan kadang tidak dilakukan oleh pihak pengirim.

Solusi lain untuk meningkatkan keamanan data didalam jaringan komputer, yaitu membuat VPN (*Virtual Private Network*), VPN dapat menghubungkan 2 atau lebih site yang berbeda secara pribadi melalui jaringan internet. VPN memiliki banyak jenis dalam aplikasinya, diantaranya adalah L2TP/IPSec.

Protokol VPN yang diimplementasikan dalam tugas akhir ini adalah L2TP/IPSec, yang merupakan protokol standar IETF (RFC 3193). Alasan

penggunaan protokol VPN ini karena L2TP / IPSec menawarkan beberapa keuntungan diantaranya mekanisme otentikasi ganda L2TP dan IPSec, virtual IP *address* yang diberikan ke *client* ketika sudah terotentikasi, serta kemudahan *client* terutama yang menggunakan sistem operasi Windows dan Mac karena sudah terdapat built-in L2TP/IPSec VPN client.

Tugas akhir ini juga menggunakan *router* sebagai gateway untuk menghubungkan jaringan local dengan jaringan internet, hal ini dikarenakan *router* juga dapat melakukan pengaturan jaringan hingga tingkat IP. Oleh karena itu dalam tugas akhir ini *router* akan digunakan sebagai VPN *server* dan VPN *client*. Router yang digunakan adalah Cisco *route*r, yang merupakan salah satu *router* yang mendukung L2TP dan IPSec.

1.2 Masalah Penelitian

1.2.1 Identifikasi Masalah

Berdasarkan uraian dari latar belakang masalah di atas maka dapat diidentifikasi permasalahan yang dapat terjadi sebagai berikut :

1. Proses implementasi yang menggunakan 2 komputer dan harus mendownload *software* tambahan.
2. Kurangnya keamanan data dalam transmisi jaringan sehingga dibutuhkan vpn untuk mengatasinya.

1.2.2 Batasan Masalah

Batasan masalah pada penelitian ini mencakup:

1. Menganalisis bagaimana proses implementasi L2TP/IPsec dalam pengiriman paket data dalam jaringan
2. Tidak membahas secara detail pengguan cara kerja algoritma enkripsi dan otentikasi
3. Tidak membahas masalah performansi jaringan.

1.2.3 Rumusan Masalah

Adapun rumusan masalah dalam penelitian ini adalah sebagai berikut :

1. Bagaimana penerapan metode L2tp/IPsec untuk optimilisasi jaringan?
2. Bagaimana cara mengamankan data dalam jaringan komputer menggunakan metode l2tp/IPsec VPN ?

1.3 Tujuan dan Manfaat Penelitian

Berdasarkan Judul dan latar belakang permasalahan yang sudah dijelaskan mengenai teknologi yang digunakan dijaringan VPN (*Virtual Private Network*) maka tujuan pembuatan dari skripsi ini sebagai berikut:

1. Memahami dan mengetahui apa itu teknologi VPN dan cara kerjanya didalam suatu jaringan.
2. Memahami dan mengetahui penjelasan teknologi IPSec *(Internet protocol security)* dan L2TP *(Layer 2 Tunneling Protocol).*
3. Mengimplementasikan L2tp/IPSec ke dalam sebuah jaringan sehingga tahu cara kerja dan pembuatannya.

BAB II
LANDASAN TEORI

2.1 Studi Perpustakaan

Abadillah (2011) dalam penelitiannya membangun sebuah *Virtual Private Server* (VPS) dan diimplemetasikan ke dalam jaringan internet Wi-Fi. Hasil penelitiannya VPN dapat dijadikan sebagai alternatif keamanan di jaringan *wireless* karena dengan VPN aliran data menjadi lebih aman. Mampu memberikan keamanan pada jaringan internet dan menanggulangi penyadapan atau pencurian *account* di jaringan internet Wi-Fi. *Remote Access* VPN dengan *Virtual Private Server* akan melakukan enkripsi terhadap data dan proses transfer data dari *Server* menuju *client* maupun sebaliknya.

Martiyanto (2011) mengimplementasikan suatu layanan *Remote Access* yang berbasiskan VPN. Implementasinya menunjukkan bahwa layanan-layanan, seperti Web *Server*, FTP *Server*, DNS *Server*, dan *server-server* lainnya, dapat berjalan dengan baik dalam lingkungan *remote access* yang berbasis VPN. *Remote Access* VPN memberikan mekanisme keamanan dengan salah satu bukti bahwa data yang dilewatkan melalui jalur VPN terbukti aman dengan tidak terdeteksinya informasi *user* dan data yang di-*request* oleh *user*.

Sarman (2006), melakukan penelitian VPN *L2TP*/*IPSec* dengan menggunakan *Open Swan* untuk membangun sebuah sistem jaringan yang digunakan untuk menghubungkan komunikasi jaringan lokal dengan jaringan publik secara aman pada penelitian yang berjudul "SERVER VPN BERBASISKAN LINUX DENGAN CLIENT WINDOWS XP SP2". Peneliti

merancang sebuah VPN pada sistem operasi *Linux Fedora* dengan menggunakan *Open Swan* dalam menerapkan *tunneling L2TP/IPSec* dan didapatkan bahwa hasil penggunaan VPN L2TP/IPSec mengakibatkan data yang saling bertukar antara klien dan *server* sudah terenkasulapsi walaupun sudah dilihat dengan *wireshark* dan juga penganalisa jaringan dari *Linux Fedora* serta oleh VPN tersebut hanya mengizinkan *user* yang memiliki kunci rahasia saja selain *username* dan *password* yang boleh melakukan pembentukan *tunnel* dengan *server* sehingga dengan VPN tersebut dapat dikatakan telah memiliki keamanan yang lebih baik.

Implementasi yang dilakukan penulis adalah dengan melakukan implementasi dan analisis paket data yang mengalir di jaringan VPN yang berbasis L2tp/IPSec. VPN yang berbasis L2tp/IPSec akan melakukan enkripsi terhadap kunci dan proses transfer data dari *server* menuju *client* maupun sebaliknya, sehingga informasi data dari *client* tidak dapat terlihat dan aman.

2.2 Dasar Teori

2.2.1 Jaringan Komputer

Jaringan komputer adalah dua atau lebih device (komputer) yang saling terhubung satu dengan yang lain dan digunakan untuk bertukar data/informasi *(sharing*), Jaringan komputer menggunakan kombinasi perangkat keras dan perangkat lunak (Sukmaaji Anjik, 2008). untuk membangun jaringan komputer, *router* dan *switch* menggunakan bermacam-macam protokol dan algoritma untuk bisa bertukar data/informasi dan membawa data menuju titik akhir yang diinginkan. Setiap titik akhir didalam jaringan mempunyai tanda pengenal yang unik.

Jaringan komputer bisa dibuat dengan menggabungkan teknologi kabel dan *wireless*. Perangkat jaringan berkomunikasi menggunakan *medium* dari transmisi *wireless* ataupun kabel. Untuk jaringan yang menggunakan transmisi kabel, membutuhkan salah satu kabel seperti kabel *coaxial*, kabel fiber optik ataupun kabel tembaga. Sementara itu, transmisi dari jaringan *wireless* termasuk jaringan komputer yang menggunakan koneksi data untuk bisa menghubungkan ke titik akhir. Titik akhir ini termasuk radio seluler, microwave, radio siaran dan satelit.

Jaringan komputer bisa dijadikan *private* atau *public*, Jaringan *private* memerlukan penggunanya untuk memasukkan *kredensial* agar bisa mengakses suatu jaringan. Biasanya, diberikan secara manual oleh administrator jaringan atau didapat langsung oleh pengguna melalui kata sandi. Jaringan *public* seperti internet yang tidak membatasi semua akses.

Didalam jaringan komputer memiliki beberapa jenis jaringan komputer, menurut Madcoms (2010) secara umum jaringan komputer dibagi menjadi 4 jenis jaringan, seperti :

1. *Local Area Network*

Local Area Network (LAN) merupakan sekumpulan komputer yang saling dihubungkan didalam satu area tertentu yang tidak begitu luas dan hanya mencakup satu wilayah local saja, seperti di dalam satu sekolah, perusahaan, kantor dan lainnya. LAN bisa juga didefinisi berdasarkan pada penggunaan alamat IP komputer didalam suatu jaringan. Suatu *host* atau komputer dapat dianggap satu LAN jika memiliki alamat IP yang

masih didalam jaringan tersebut, sehingga tidak membutuhkan router ataupun device lain untuk berkomunikasi.

Jaringan LAN dibagi menjadi dua tipe, yaitu jaringan *client-server* dan jaringan *peer to peer*. Pada jaringan *client-server*, satu komputer bertindak sebagai *workstation* dan komputer lain sebagai *server*, sedangkan didalam jaringan *peer to peer*, setiap komputer yang terhubung didalam jaringan dapat bertindak baik sebagai *workstation* maupun *server*.

2. *Metropolitan Area Network*

Metropolitan Area Network (MAN) merupakan jaringan komputer yang dapat mencakup area yang lebih luas dibandingkan LAN, contohnya menghubungkan jaringan komputer dari satu kota kekota lainnya, MAN juga menggunakan teknologi yang lebih canggih dari semua jaringan komputer yang ada pada LAN. MAN mampu menunjang data dan suara, bahkan juga bisa berhubungan dengan jaringan televisi kabel.

3. *Wide Area Network*

Wide Area Network (WAN) merupakan salah satu jenis jaringan komputer yang wilayahnya sangat luas bukan meliputi satu kota kekota lain dalam suatu wilayah, tetapi menjangkau area atau wilayah otoritas negara lain. Jaringan MAN biasanya sudah menggunakan media *wireless*, kabel serat optik, ataupun sarana satelit.

WAN biasanya lebih rumit dibandingkan MAN maupun LAN. Karena banyak menggunakan sarana agar bisa menghubungkan antara LAN dan WAN kedalam komunikasi global contohnya internet, meski demikian antara WAN, MAN dan LAN tidak banyak berbeda dalam banyak hal, hanya areanya yang berbeda satu diantara yang lainnya.

4. *Internet dan Intranet*

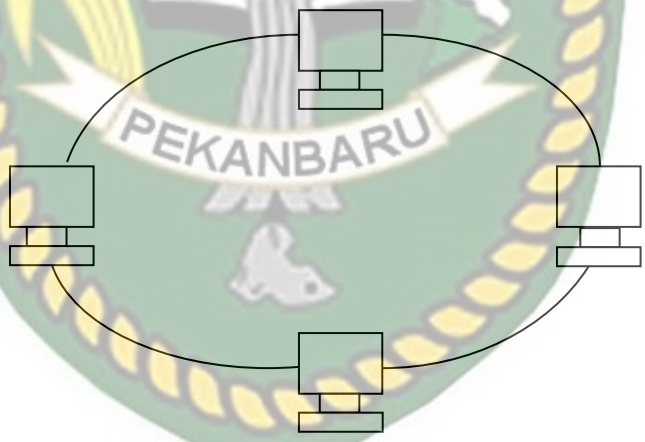
Internet merupakan gabungan beberapa jenis jaringan komputer, internet adalah suatu jaringan komunikasi global yang menghubungkan satu media elektronik (komputer, ponsel dan lainnya) dengan media elektronik lainnya dan menghubungkan jaringan-jaringan komputer di seluruh dunia. Setiap media elektronik dan jaringan terhubung secara langsung ataupun tidak langsung ke dalam jalur utama (*internet backbone)* dan dibedakan dari satu dengan yang lainnya menggunakan alamat unik yang disebut dengan alamat *Internet Protocol* (IP).

Didalam jaringan *internet* dapat juga diterapkan aplikasinya kedalam sebuah jaringan LAN yang mempunyai *server*. Seperti contoh perusahaan yang mempunyai jaringan *client-server*. Apabila aplikasi yang ada didalam *internet*, seperti *mail server*, diterapkan pada perusahaan tersebut, jaringan itu sendiri bisa disebut sebagai *intranet*. *Client* bisa mengakses *server* seperti mengakses *internet* pada umumnya. *Client* bisa juga mengakses aplikasi lain di luar *server* dari perusahaan tersebut.

Dalam jaringan komputer juga mempunyai topologi, topologi mengacu pada tata letak perangkat yang terhubung. Topologi bisa dibilang sebagai bentuk atau struktur *virtual* jaringan, Topologi jaringan dikategorikan ke dalam tipe dasar berikut:

1. Topologi *Ring*

Topologi *ring* menghubungkan semua komputer dan membentuk sebuah pola lingkaran sehingga disebut *ring*, topologi ring menghubungkan dari *host* ke *host* sebelum ataupun setelahnya, topologi *ring* berkomunikasi menggunakan data token agar bisa mengontrol hak akses dari komputer agar bisa menerima data.

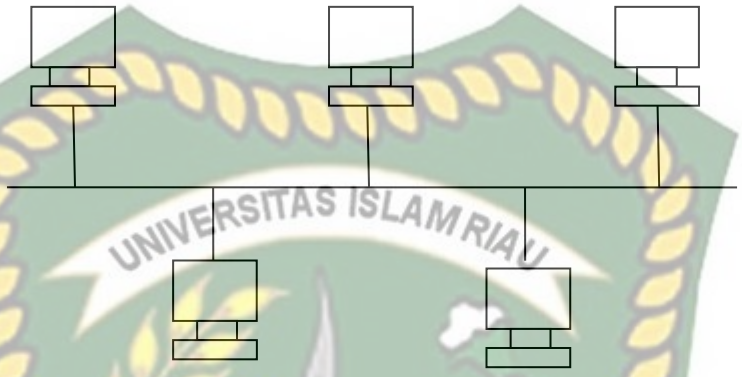


Gambar 2.1 Topologi *Ring*

2. Topologi *Bus*

Topologi *bus* hanya menggunakan satu kabel yaitu kabel coaxial yang disusun rapi seperti antrian dan terhubung ke kabel menggunakan

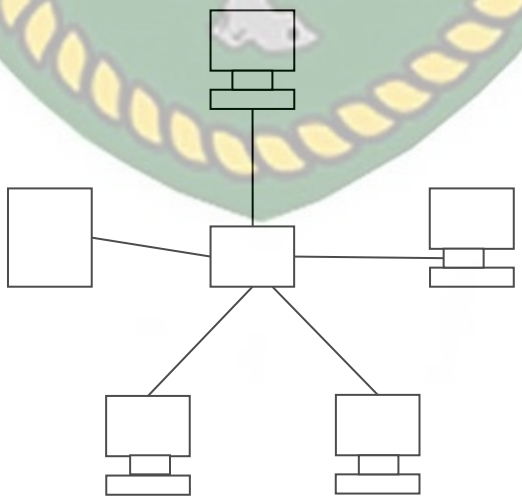
konektor BNC dari setiap komputernya, dan dari dua ujung kabel coaxial harus diakhiri menggunakan terminator.



Gambar 2.2 Topologi *Bus*

3. Topologi *Star*

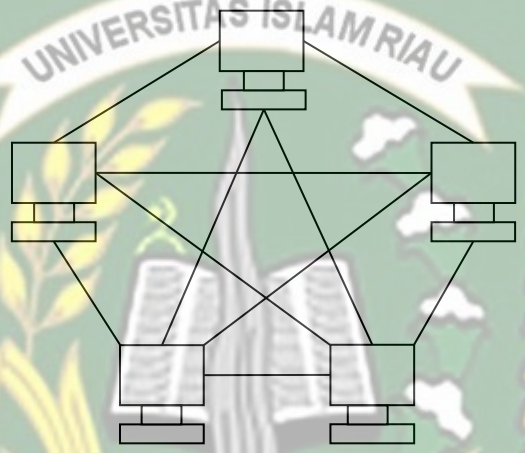
Topologi *star* membentuk seperti bintang karena semua komputer di hubungkan ke sebuah *hub* atau *switch* dengan kabel UTP, sehingga *hub*/*switch* lah pusat dari jaringan dan bertugas untuk mengontrol lalu lintas data.



Gambar 2.3 Topologi *Star*

4. Topologi *Mesh*

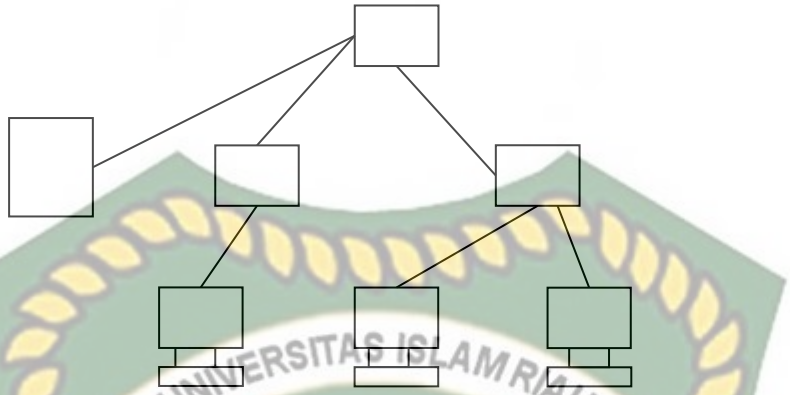
Pada topologi ini setiap komputer akan terhubung dengan komputer lain dalam jaringannya menggunakan kabel tunggal, jadi proses pengiriman data akan langsung mencapai komputer tujuan tanpa melalui komputer lain atau pun *switch* atau *hub*.



Gambar 2.4 Topologi *Mesh*

5. Topologi *Tree*

Topologi *Tree* merupakan sebuah topologi jaringan komputer yang menggabungkan dari topologi *star* yang dihubungkan dengan topologi *bus*, dalam penyusunannya topologi bus digunakan sebagai tulang punggung dari setiap topologi *star* yang terhubung ke topologi *star* lainnya, topologi tree ini juga disebut dengan topologi bertingkat, terdapat banyak macam tingkatan jaringan ditopologi tree, jaringan yang berada pada tingkat yang tinggi dapat mengontrol jaringan yang berada pada tingkat yang rendah.



Gambar 2.5 Topologi *Tree*

2.2.2 Perangkat Jaringan

Masih dalam bukunya, Madcoms (2010) menjelaskan tentang perangkat jaringan merupakan semua komputer, perangkat tambahan, *interface card*, dan juga *peripheral* yang saling terhubung di dalam suatu jaringan komputer agar bisa melakukan transformasi data. Perangkat jaringan terdiri dari:

1. *Server*

Server merupakan pusat control untuk mengakses jaringan komputer yang terdapat sumber daya didalamnya, seperti berkas ataupun alat pencetak (printer), dan memberikan akses kepada anggota workstation dijaringan. *Server* berfungsi untuk menyimpan data atau informasi dan juga untuk mengelola suatu jaringan komputer.

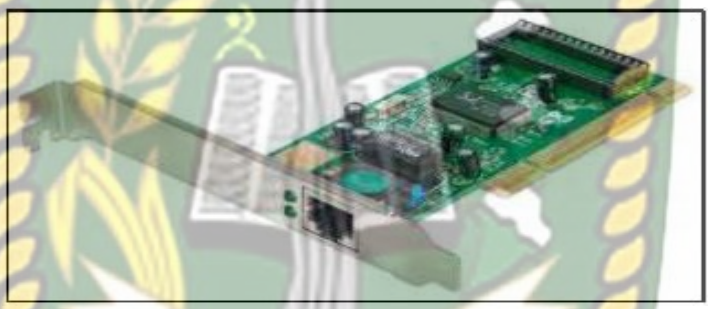
2. *Workstation*

Workstation merupakan komputer yang sudah terhubung didalam sebuah jaringan LAN, menjalankan *multi-user operating system*, komputer yang sudah

terhubung didalam jaringan disebut sebagai *workstation*. *Workstation* menjadi terminal untuk setiap komputer yang melakukan transfer data antar komputer.

3. *Network Interface Card*

Network Interface Card bisa juga disebut sebagai kartu jaringan adalah suatu kartu yang mempunyai fungsi agar komputer dapat terhubung didalam suatu jaringan komputer dengan menggunakan kabel jarirngan. NIC juga sering disebut dengan LAN *card*.



Gambar 2.6 *Network Interface Card*

4. Kabel

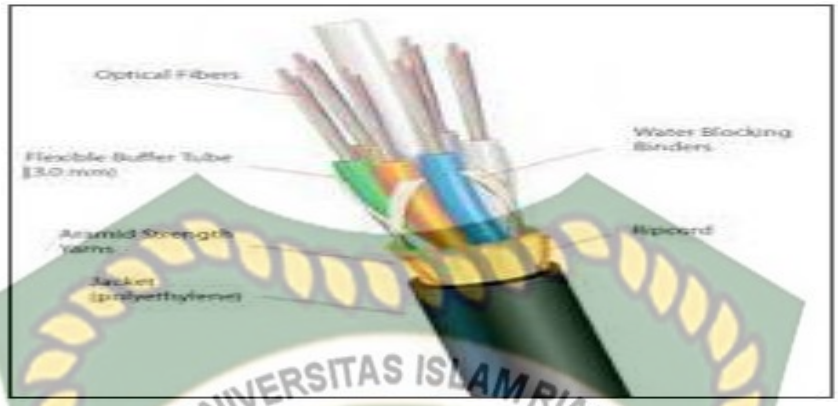
Kabel didalam sebuah jaringan digunakan sebagai media yang menghubungkan antara dua *workstation* atau lebih. Kabel mempunyai banyak jenis, kabel yang digunakan didalam jaringan adalah kabel *twisted pair*, *coaxial*, dan *fiber optic*.

Kabel *coaxial* terdiri dari kawat tembaga sebagai inti dan berada ditengah, yang berfungsi sebagai pengantar aliran listrik, lapisan plastik yang berfungsi sebagai pembatas antara kawat tembaga dan lapisan metal. Kabel *coaxial* mempunyai kecepatan transfer sampai 10 *Mbps*. Kabel *coaxial* sering digunakan untuk penyambung televisi dan anthena, instalasi cctv, jaringan

LAN, *thick ethernet* dan *thin ethernet*. Kabel ini secara fisik berat dan tidak fleksibel, namun jangkauannya dan kecepatan transmisi yang dimilikinya lebih tinggi, meskipun masih ada beberapa batasan-batasan jangkauan tertentu. Kabel *coaxial* biasanya digunakan didalam jaringan topologi bus yang dimana titik percabangannya menggunakan *TConnector* dan juga menggunakan konektor BNC untuk mengkoneksi setiap nodenya.

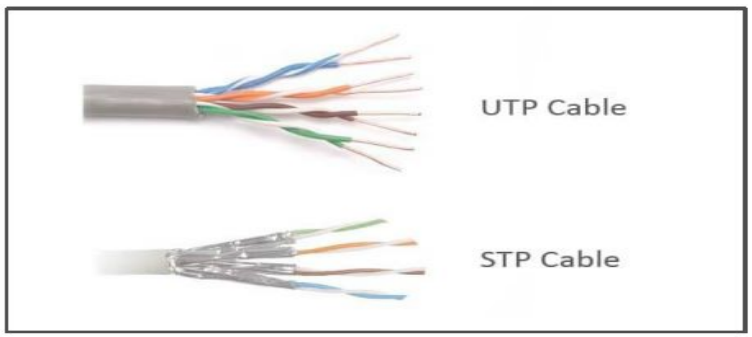
Gambar 2.7 Kabel *Coaxial*

Kabel fiber optic adalah sebuah kabel yang terbuat dari serat kaca yang dilindungi oleh beberapa lapisan pelindung. Kabel fiber optic dibuat dengan teknologi canggih sehingga memiliki kecepatan untuk pengiriman data, Pengirimannya menggunakan sinar atau bias cahaya. Kabel fiber optik memiliki jarak yang lebih jauh daripada kabel *coaxial* dan *twisted pair*, dan memiliki dua tipe, yaitu *single mode* dan *multi mode*. Kabel ini juga memiliki kecepatan transfer data mencapai 155 Mbps.



Gambar 2.8 Fiber Optik

Kabel *twisted pair,* terdiri dari kabel yang saling melilit dan dibagi menjadi 2 tipe, *Unshilded Twisted Pair* (UTP) dan *Shielded Twisted Pair* (STP), kabel twisted pair memiliki pasangannya sendiri yang terdiri dari dua, empat ataupun lebih. Fungsi *twist* (melilit) bertujuan untuk mengurangi medan magnet atau terhadap kabel lain. Kecepatan transfer data yang dapat dilayani sampai 10 Mbps. Jenis konektor yang biasa digunakan adalah konektor seri *registered jack* (RJ), RJ memiliki 2 jenis yaitu RJ-11 digunakan untuk kategori 2 sampai 4 atau RJ-45 untuk kategori 5 keatas. Dari kedua tipe kabel *twisted pair* ini, tipe UTP sering digunakan didalam jaringan LAN. Perangkat yang dipakai didalam penggunaan jenis kabel UTP yaitu konektor RJ45, *Switch* atau *hub*.



Gambar 2.9 Kabel STP dan UTP

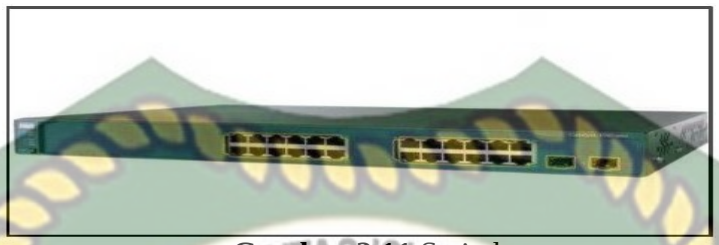
5. *Hub* dan *Switch*

Hub adalah perangkat jaringan dengan banyak *port Ethernet* yang digunakan untuk menghubungkan dua komputer atau lebih didalam sebuah jaringan komputer sehingga bisa melakukan komunikasi data maupun pertukaran data atau informasi. Perangkat yang terhubung pada port akan tersambung didalam sebuah jaringan LAN. *Hub* bekerja dengan metode *broadcast,* sebagai penerima sinyal dari satu perangkat komputer dan akan mentransmisikan keperangkat komputer lainnya yang terhubung didalam semua *port* nya. *Hub* berada didalam *physical layer*.

Gambar 2.10 Hub

Switch merupakan sebuah perangkat jaringan pada komputer yang berfungsi untuk menghubungkan perangkat didalam jaringan komputer dengan menggunakan pertukaran paket untuk mengirim, memproses dan menerima data dari satu komputer menuju kekomputer lainnya ataupun sebaliknya. *Switch* dan hub memiliki perbedaan didalam pengiriman data, switch mengirim data ke port yang memang menjadi tujuannya, sedangkan pada hub data yang diterima akan

secara otomatis mengirim data keseluruh perangkat yang terkoneksi didalam jaringan tersebut.



Gambar 2.11 Switch

6. *Bridge*

Bridge adalah suatu alat yang dapat menghubungkan jaringan yang berbeda atau menjembataninya. Maksudnya dapat mengkoneksi tipe jaringan komputer yang berbeda-beda (seperti *fast Ethernet* dan *Ethernet*), menggabungkan lebih dari satu jaringan local (menghubungkan jaringan LAN dengan jaringan LAN yang lain), menggabungkan dua buah jaringan atau sebagai pemecah sebuah jaringan yang besar dan dijadikan beberapa jaringan kecil untuk meningkatkan performa jaringan tersebut, dan juga bisa menghubungkan diantara network yang berbeda tipe kabel ataupun topologi berbeda juga.

Gambar 2.12 *Bridge*

7. *Router*

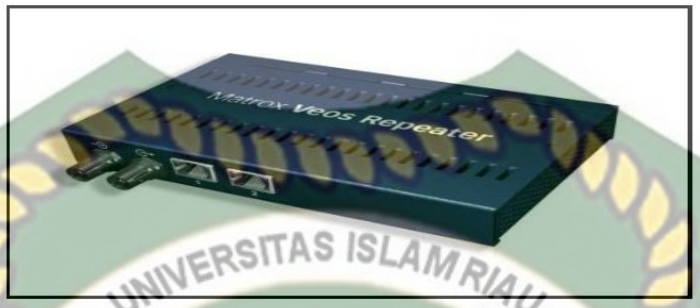
Router adalah sebuah perangkat yang digunakan untuk menganalisis dan mengirim paket data yang sudah dianalisis dari satu jaringan menuju kejaringan lain, *router* juga berfungsi menghubungkan jaringan LAN menuju *internet working* atau WAN dan mengelola komunikasi lalu-lintas data yang ada di dalamnya, dan mencari jalur terbaik untuk komunikasi data. *Router* berada pada lapisan 3 model jaringan OSI yaitu pada lapisan *network*. Yang dimana memindahkan paket-paket antar jaringan menggunakan alamat logikanya.

Gambar 2.13 *Router*

8. *Repeater*

Repeater merupakan sebuah alat atau komponen jaringan yang berfungsi untuk memperkuat sinyal yang diterima dari satu jaringan menuju jaringan berikutnya dan akan dipancarkan lagi dengan kecepatan yang sama dari sinyal yang asli sehingga jarak antara dua komputer dapat diperluas, dan juga bisa dikatakan repeater berfungsi untuk memperkuat atau meregenerasi sinyal-sinyal yang masuk. *repeater* bekerja didalam lapisan *physical layer* dalam

model jaringan *OSI*. *Repeater* mempunyai dua macam *system* untuk meningkatkan frekuensi dari data yaitu *system* analog dan *system* digital.



Gambar 2.14 *Repeater*

9. *Modem*

Modem adalah sebuah perangkat yang digunakan sebagai penghubung jaringan LAN dari komputer menuju jaringan ke Penyedia Layanan Internet *(Internet Service Provider /ISP)*. Salah satu modem yang sering digunakan untuk menghubungkan ke internet yaitu *modem ADSL*.

Gambar 2.15 *Modem*

2.2.3 TCP/IP

TCP/IP adalah protokol standar yang digunakan untuk komunikasi data antar komputer dimana terjadi proses tukar-menukar data *(Sharing)* dari satu

komputer menuju ke komputer lain di dalam sebuah jaringan *Internet* (Sofana Iwan, 2004). TCP/IP merupakan *protocol suite* (banyak bagian), dan tidak bisa berdiri sendiri. *Protocol* adalah prosedur atau tugas yang harus dilakukan agar beberapa komputer dapat saling berkomunikasi.

Protokol TCP/IP mempunyai beberapa layer dengan tugas dan tanggung jawab masing-masing untuk mengolah data baik yang diterima maupun data yang akan dikirim, standart layer utama dari TCP/IP yaitu *application layer*, *transport layer*, *network layer* atau *internet layer*, dan *physical layer.*

Application layer adalah lapisan paling atas yang terdapat disistem TCP/IP yang berfungsi untuk menyediakan *interface* atau antar muka aplikasi yang digunakan sebagai komunikasi didalam jaringan, *transport layer* merupakan lapisan yang memiliki tugas sebagai pengantar data atau paket, *network layer* adalah lapisan yang bekerja didalam tingkat 5, merupakan lapisan penting dalam proses transmisi jaringan komputer, sedangkan physical layer merupakan lapisan yang berhubungan dengan fisik dan berhubungan dekat dengan perangkat keras jaringan.

2.2.4 IP Address

IP address adalah alamat logika yang diberikan ke peralatan jaringan menggunakan protokol TCP/IP. *IP address* terdiri dari 32 bit angka *binary*, yang ditulis dalam empat kelompok yang masing-masing kelompoknya terdiri dari 8 *bit (oktat)* yang dipisah oleh tanda titik. Seperti :

11000000.00010000.00001010.00000001

Atau juga bisa ditulis dalam bentuk 4 kelompok format *desimal* (0-255), misalnya:

192.16.10.1

IP address yang terdiri dari 32 bit angka disebut sebagai (IPv4) atau IP versi 4. *IP address* terdiri dari *network* ID dan *host* ID. Dimana *network* ID menentukan alamat jaringan, sedangkan *host* ID menentukan alamat *host* atau komputer. Berapa jumlah *network* ID ataupun *host* ID tergantung didalam kelas *IP address* yang dipakai.

IP address dapat dibedakan menjadi lima kelas, yaitu kelas A, kelas B, kelas C dan kelas D. kelas A, kelas B dan kelas C digunakan sebagai *address* biasa. Sedangkan kelas D digunakan sebagai *multicasting.* Berikut penjelasan masing-masing kelas *IP address*:

1. Kelas A

   Kelas ini dibangun untuk mengsupport *network* yang sangat besar memiliki jumlah lebih dari 16 juta alamat *host*. Kelas ini memakai oktet pertama untuk menampilkan alamat jaringan, tiga oktet berikutnya tersedia untuk alamat *host*.

   Bit pertama dari oktat pertama kelas A adalah 0, dengan demikian maka *range* yang bisa didapatkan adalah 0-127 dalam bilangan biner atau 00000000-01111111. Tetapi untuk angka 0 dan 127 tidak dapat digunakan. Serta *IP address* 127.0.0.0 khusus digunakan untuk *loopback testing*. Maka

angka dari oktet pertama yang merupakan nilai dari 1 sampai 126 yaitu *address* kelas A.

2. Kelas B

Kelas ini dibangun untuk kebutuhan jaringan skala menengah hingga besar. Kelas ini menggunakan dua oktet pertama untuk menampilkan alamat jaringan, dua oktet berikutnya tersedia sebagai alamat.

Dua *bit* pertama dari oktet pertama kelas B adalah 10, dengan demikian maka *range* yang bisa didapatkan adalah 128-191 dalam bilangan biner atau 10000000-10111111. Maka angka dari oktet pertama yang merupakan nilai dari 128 sampai 191 adalah *address* kelas B.

3. Kelas C

Kelas ini banyak digunakan untuk mengsupport jaringan skala kecil dengan jumlah maksimum *host* per networknya adalah 254 host.

Tiga *bit* pertama dari oktet pertama kelas C adalah 110, dengan demikian maka *range* yang bisa didapatkan adalah 192-223 dalam bilangan biner atau 11000000-11011111. Maka angka dari oktet pertama yang merupakan nilai dari 192 sampai 223 adalah *address* kelas C.

4. Kelas D

Kelas ini digunakan untuk *multicasting*, yaitu alamat jaringan yang unik menampilkan paket dengan alamat tujuan ke *group predefined*

dari sebuah IP *address*. Oleh karena itu *single unit* dapat mentransmit aliran tunggal dari data secara simultan ke lebih dari satu penerima.

Empat *bit* pertama dari oktet pertama kelas D adalah 1110, dengan demikian maka *range* yang bisa didapatkan adalah 224-239 dalam bilangan biner atau 11100000-11101111. Maka angka dari oktet pertama yang merupakan nilai dari 224 sampai 239 adalah alamat kelas D.

Tabel 2.1. Tabel IP *Address*

Kelas IP	Range	First Network ID	Last Network ID	Default Subnet Mask	Max Usable Host Per Network ID
Kelas A	1 - 126	1.0.0.0	126.0.0.0	255.0.0.0	16777216
Kelas B	128 - 191	128.0.0.0	191.255.0.0	255.255.0.0	65536
Kelas C	192 - 223	192.0.0.0	233.255.255.0	255.255.255.0	254
Kelas D	224 - 239	Digunakan untuk keperluan Multicasting.			
Kelas E	240 - 255	Digunakan untuk keperluan pengembangan (research and experiment)			

2.2.5 *Routing*

Routing dibedakan menjadi dua jenis, yaitu *routing* statis (*static routing*) dan r*outing* dinamis (*dynamic routing*) (saputra dkk, 2015:3).

1. *Routing* Statis

Routing statis mempunyai pengaturan paling sederhana yang dapat dilakukan pada jaringan komputer. Administrator jaringan hanya mengisi setiap entri dalam *forwarding table* di setiap router yang ada di jaringan tersebut.

2. Routing Dinamis

Routing dimana router dapat menentukan sendiri rute terbaik yang akan dilaluinya dalam meneruskan sebuat paket dari network satu ke network lainnya. Administrator jaringan hanya menentukan bagaimana router mempelajari paket.

Rute pada *routing* dinamis dapat berubah sesuai dengan pelajaran yang didapat oleh router.

2.2.6 VPN

VPN adalah singkatan dari "Virtual Private Network", VPN adalah suatu koneksi atau suatu cara membuat suatu jaringan dengan jaringan lain bersifat private melalui jaringan internet (*public*). Pengguna dapat mengirim dan menerima data didalam jaringan *public* tanpa diketahui oleh pengguna lain, karena data tersebut melewati *tunnel* yang dibuat oleh VPN. *Tunnel* merupakan suatu system untuk deskripsi dan enkripsi untuk sebuah data. Data yang ditransfer difragmentasi menjadi paket yang lebih kecil dan melewati terowongan (tunnel) sehingga data menjadi lebih aman. (Sunyoto Wendy Aris, 2006).

VPN memiliki dua bagian penting, antara lain VPN *Server* dan VPN *Client*, yang mana VPN *Server* bertugas sebagai penyedia layanan *tunneling* bagi *client* dan sebaliknya. *Client* adalah host yang memakai jasa VPN *Server* yang tujuannya agar dapat terhubung dengan jaringan VPN tersebut. VPN *Server* ini dapat berupa komputer dengan aplikasi VPN *server* atau sebuah *router*.

Fungsi utama VPN adalah *confidentially* (kerahasiaan), data yang dikirim akan dienkripsi dan yang diterima akan didekripsi. Data *Intergrity* (keutuhan data), VPN akan menjaga data dari mulai data tersebut dikirim oleh pengirim hingga data sampai ditempat penerima. VPN akan melakukan pemeriksaan dari semua data yang masuk dan mengambil informasi dari sumber datanya. Sehingga, VPN bisa menjamin data yang dikirim dan diterima berasal dari sumber yang seharusnya. *Non-repudiation*, yaitu mencegah dua pihak dari menyangkal bahwa

mereka telah mengirim atau menerima sebuah file dengan mengakomodasi perubahan. Dan yang terakhir kendali akses, yaitu menentukan siapa yang diberikan akses ke sebuah sistem atau jaringan, sebagaimana informasi apa dan seberapa banyak seseorang dapat menerima. VPN merupakan media komunikasi khusus yang sangat efisein didalam jaringan *public (internet)* walaupun VPN beroperasi pada topologi yang berbeda dan lebih sulit dari pada jaringan *point to point.*

Gambar 2.16 Gambaran VPN

Pada gambar 6, untuk memulai sebuah komunikasi, komputer VPN *Client* mememanggil VPN *Server* dan memeriksa *username* dan *password*. Apabila *username* dan *password* benar, VPN *Server* akan mengirim *IP Address* baru pada komputer *client* untuk membuat sebuah koneksi, sehingga *tunnel* akan terbentuk. komputer *client* dapat mengakses berbagai sumber daya (komputer atau jaringan LAN) yang berada didalam VPN *Server*, misalnya melakukan cetak dokumen, pengiriman data, *browsing*, dan melakukan *remote desktop*.

2.2.7 L2TP

L2TP atau singkatan dari "*layer 2 tunneling protocol*" merupakan standar dari IETF *(Internet Engineering Task Force)* yang berfungsi untuk masalah *protocol tunneling* untuk mengencapsulasi dan menggantikan frame dari protocol PPTP. L2TP adalah penggabungan dari dua teknologi yaitu *Microsoft* PPTP dengan *Layer* 2 *Forwarding* (L2F) protokol *tunneling* Cisco (Sunyoto Wendy Aris, 2006). Selain jaringan IP, L2TP juga bisa *tunneling* melalui berbagai jenis jaringan *point-to-point* kemudian ditransmisikan melalui jaringan TCP/IP X.25, termasuk *Frame Relay* dan ATM.

L2TP tidak benar-benar bisa mengenkripsi sebuah data sama halnya dengan protocol PPTP, L2TP juga tidak dapat mengotentikasi pesan individu. Untuk mengatasi kekurangan ini, L2TP sering dihubungkan dengan IPSec. penggabungan ini memberikan lapisan tambahan otentikasi dan enkripsi. karena paket-paket L2TP digabungkan didalam suatu paket IPSec pada lapisan jaringan. L2TP beroperasi didalam *layer Data-Link* dari model OSI dan memakai port UDP 1701.

Gambar 2.17 Protocol L2tp

2.2.8 IPSEC

IPsec atau singkatan dari *"IP Security"* merupakan sebuah protocol jaringan yang digunakan untuk transmisi diagram disebuah *internetwork* berbasis TCP/IP. IPsec bisa juga didefinisikan satu kerangka kerja dari protokol- protokol untuk keamanan pada jaringan atau melakukan enkripsi dan integritas data dilapisan kedua atau *internetwork layer* (Sunyoto Wendy Aris, 2006). Keuntungan yang ada di IPSec adalah struktur keamanannya dapat diatasi tanpa memerlukan perubahan pada pemakai individual. Cisco menjadi pemimpin dalam mengusulkan IPSec sebagai suatu standar yang bisa mencakup dukungan dirouternya. IPSec menyediakan layanan kriptografi untuk keamanan transmisi data.

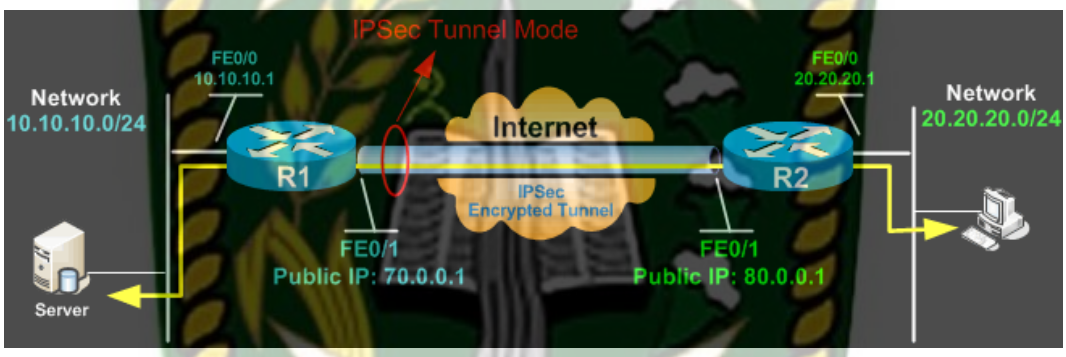
IPsec juga mempunyai layanan lain diantaranya *authenticity, integrity, access control, confidentiality,* dan *anti replay*. Layanan IPSec hanya melayani lapisan pada jaringan, dan dilakukan secara transparan. Layanan tersebut diantaranya sebagai berikut:

A. *Confidentiality*, untuk meyakinkan bahwa sulit untuk dimengerti orang lain tetapi mudah dimengerti oleh penerima bahwa data sudah dikirimkan. Contoh: Kita tidak ingin seseorang mengetahui *password* ketika *login* ke *remote server*.
B. *Integrity*, untuk menjamin bahwa data yang dikirim tidak akan berubah dalam perjalanan menuju tempat tujuan.
C. *Authenticity*, untuk menandai bahwa data yang dikirimkan memang berasal dari pengirim yang benar.
D. *Anti Replay*, untuk meyakinkan bahwa transaksi di IPsec hanya dilakukan sekali dan tidak dikirim berulang kali (replayed), kemudian data tersebut

akan ditransmisikan lagi melalui jaringan *internet* tanpa harus takut data akan di modifikasi oleh pihak yang tidak berwenang untuk mengakses.

IPSec bekerja didalam tiga bagian, yaitu:

1. *Network-to-network*
2. *Host-to-network*
3. *Host-to-host*



Gambar 2.18 *Protocol Ipsec*

BAB III

METODOLOGI PENELITIAN

Metodologi penelitian sebuah cara atau proses peneliti untuk mendapatkan data atau informasi yang digunakan untuk keperluan penelitian. Metodologi juga merupakan analisis teoretis mengenai suatu cara atau metode. Penelitian merupakan suatu penyelidikan yang sistematis untuk meningkatkan sejumlah pengetahuan, juga merupakan suatu usaha yang sistematis dan terorganisasi untuk menyelidiki masalah tertentu yang memerlukan jawaban.

Penelitian bisa dipahami dengan mempelajari berbagai aspek yang berbeda sehingga akan mendorong peneliti untuk melakukan penelitian. Keinginan untuk memperoleh dan mengembangkan pengetahuan merupakan kebutuhan dasar manusia yang umumnya menjadi motivasi untuk melakukan penelitian.

3.1 Alat dan Bahan Penelitian

Untuk melengkapi kebutuhan penelitian diperlukan Alat dan Bahan Penelitian sebagai pelengkap agar mudah dalam melanjutkan kegiatan penelitian tersebut, adapun alat dan bahan penelitian sebagai berikut :

3.1.1 Alat Penelitian

Adapun spesifikasi Perangkat Keras *(Hardware)* dan Perangkat Lunak *(Software)* yang di gunakan untuk melakukan simulasi pengujian Implementasi *L2tp/IPsec* menggunakan *Router* Cisco yang akan di bangun yaitu sebagai berikut:

3.1.1.1 Spesifikasi Perangkat Keras *(Hardware)*

Adapun spesifikasi Perangkat Keras *(Hardware)* yang akan di gunakan dalam penelitian ini adalah :

Tabel 3.1 Spesifikasi Perangkat Keras *(Hardware)*

No	Perangkat Keras *(Hardware)*	Spesifikasi/Keterangan	Fungsi/Kegunaan
1	PC/Client	• Procesor Intel Core i3. • RAM 2 GB. • *Harrdisk* 500 GB. • Tipe Sistem 64 bit atau 32 bit *Operating System*. • 1 Unit Pc Client	Digunakan sebagai Pc Client pada Desain Jaringan.
2	PC/Laptop	• Procesor Intel Core i5. • RAM 4 GB. • *Harrdisk* 500 GB. • Tipe Sistem 64 bit atau 32 bit *Operating System*. • 1 Unit Pc Laptop	Digunakan sebagai Pc konfigurasi Desain Jaringan dan Server
3	Kabel Unshield Twisted Pair(UTP).	6 buah.	Digunakan untuk menghubungkan antara *Router, Switch*, dan Pc Client.
4	Router Cisco	3 Unit Type 2900	Digunakan untuk konfigurasi routing Eigrp dan menghubungkan ke Pc Client.

3.1.1.2 Spesifikasi Perangkat Lunak *(Software)*

Sistem Operasi : *Microsoft Windows* 7 32 bit

Packet Tracer : Aplikasi simulasi dan desain jaringan komputer.

Putty : Remote console/ terminal yang digunakan untuk meremote komputer dengan terhubungnya menggunakan port ssh atau sebagainya pada Cisco Router.

Snipping tool : Aplikasi yang digunakan untuk mengambil gambar dari layar monitor pc ataupun laptop

3.1.2 Bahan Penelitian

Pengumpulan data merupakan langkah penting untuk mendapatkan data yang benar dan meyakinkan agar hasil yang didapat tidak menyimpang dari tujuan yang diharapkan sebelumnya, adapun langkah-langkah penulis dalam melakukan penelitian sebagai berikut :

a. Analisa

Metode awal dalam melakukan penelitian yaitu Analisa, Analisa digunakan untuk menganalisa sebuah rancangan yang dibangun pada pembuatan suatu desain jaringan, mulai dari tahap rancang bangun desain jaringan, hingga pengujian jaringan tersebut apakah hasil yang didapat dari rancangan yang di implementasikan akan mendapatkan hasil yang baik.

b. Perancangan

Metode kedua yaitu perancangan, pada tahap ini akan menerapkan yang telah didapat pada tahap awal "Analisa" kedalam bentuk desain jaringan untuk di implementasikan kedalam sistem jaringan komputer.

c. Pengujian

Metode ketiga yaitu pengujian, pada tahap ini pengujian dilakukan pada komputer Client, router Cisco untuk menunjukkan jika desain jaringan yang akan di terapkan bekerja dengan baik.

d. Dokumentasi

Metode keempat yaitu dokumentasi, pada tahap ini proses dokumentasi, penulis melakukan tinjauan pustaka, membaca dan mempelajari buku-buku, serta mencari dari sumber-sumber yang berkaitan dengan penelitian untuk dijadikan sebagai bahan referensi.

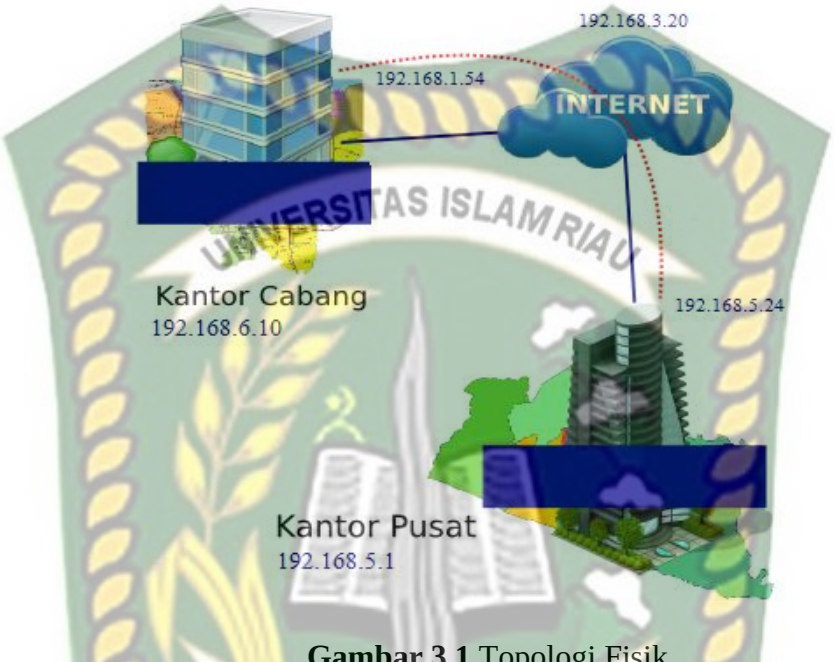
3.2 Perancangan Sistem

Perancangan Sistem Melalui beberapa tahapan yaitu Perancangan Jaringan dan Desain Konfigurasi Router, Perancangan Jaringan meliputi desain topologi jaringan, desain konfigurasi router meliputi setting IP *Address* dan *Routing* pada *router*, adapun tahapan-tahapan tersebut sebagai berikut :

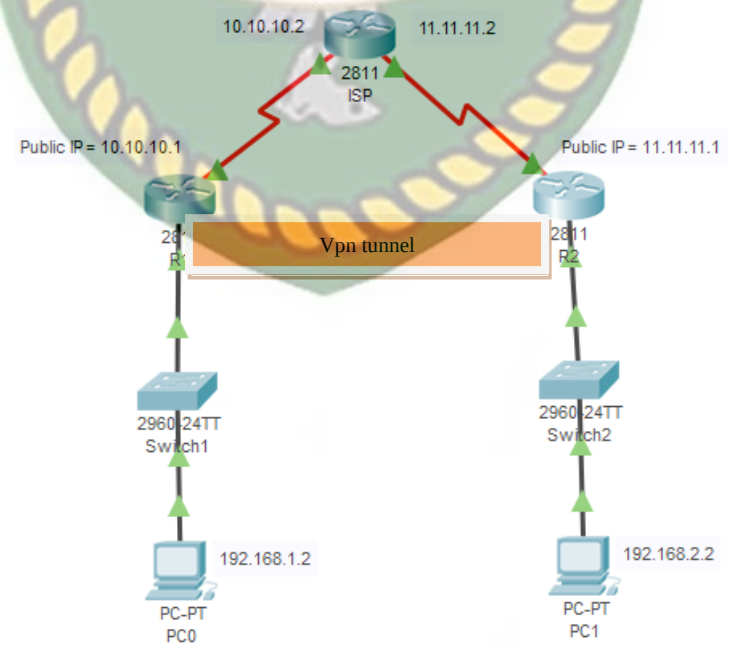
3.2.1 Perancangan Jaringan

Pada penerapan jaringan ini menggunakan jaringan lokal yang terdiri dari 1 PC sebagai Client dengan sistem operasi *windows* 7 dilengkapi dengan Cisco

Packet Tracer untuk mendesain bentuk rancang bangun jaringan. Topologi yang akan diterapkan yaitu :



Gambar 3.1 Topologi Fisik



Gambar 3.2 Topologi *logic*

3.2.2 Desain Konfigurasi Router

Pada desain ini akan menggambarkan pengalamatan router pada jalur IP Address yang sudah di tentukan agar lebih mempermudah dalam melakukan pengaturan konfigurasi jaringan, untuk Ipv4 sudah didapatkan dari koversi pada tunnel broker pada tabel 3.2 dibawah ini :

Tabel 3.2 IP Address *Router Cisco 2900*

Router	Interface	IP Address	Subnet Mask	Gateway
Pc Server	-			
		192.168.1.2	255.255.255.0	192.168.1.1
R1	Eth1 / G0/1		-	-
		192.168.1.1	255.255.255.0	-
	Eth2 / G0/0		-	-
		10.10.10.1	255.255.255.0	
R2	Eth1 /G0/1		-	-
		192.168.2.1	255.255.255.0	-
	Eth2 / G0/0		-	-
		11.11.11.1	255.255.255.0	-
R3	Eth1 /G0/0		-	-
		10.10.10.2	255.255.255.0	-
	Eth2 / G0/1		-	-
		11.11.11.2	255.255.255.0	-
Pc Client	-		-	-
		192.168.2.2	255.255.255.0	192.168.2.1

Setelah alamat IP Address ditentukan pada router, selanjutnya memberikan pengalamatan IP *Routing* Eigrp untuk *router Cisco* pada setiap *routernya*, dan *routing static* pada *Router* untuk pengalamatan IP *Routing* dapat dilihat pada tabel dibawah ini:

Tabel 3.3 *Routing* untuk Router Cisco 2900

Router	IP Address	EIGRP Area
R1	10.10.10.2	Backbone
R2	11.11.11.2	Backbone
R3	192.168.1.0/24	Backbone
	192.168.2.0/24	Backbone

3.3 Skenario yang digunakan pada Simulasi

Dari topologi diatas dapat dilihat koneksi yang akan dihubungkan dari *Server* ke *client* akan melewati beberapa *router*. Kemudian akan diproses melalui routing pada router yang telah di konfigurasi sebelumnya dan diteruskan ke *client* melalui *Switch*.

Protokol *routing* adalah salah satu komponen penting pada *network* TCP/IP. Protokol *routing* secara dinamis berkomunikasi untuk menentukan rute terbaik mencapai tujuan. Paket di-*forward* dari satu *route* ke *route* yang lain.(Sofana, Iwan. 2012).

3.4 Prosedur Penelitian

Implementasi *L2tp/Ipsec* Menggunakan *Cisco Router* dengan *Routing OSPF* ini melalui beberapa tahapan-tahapan yang akan dijadikan prosedur penelitian, adapun tahapan prosedur penelitian sebagai berikut :

3.4.1 Skema Rancangan Program Penelitian

Prosedur penelitian pertama yaitu Skema Rancangan Penelitian yang mana mulai dari Perancangan Topologi meliputi desain jaringan , Konfigurasi Jaringan seperti *Setting IP Address Routing IP Address,* Simulasi Koneksi Jaringan seperti menjalankan koneksi jaringan yang telah di desain, Uji Coba Jaringan melakukan Test pada koneksi jaringan dengan aplikasi monitoring jaringan, Analisa dan Hasil untuk melihat hasil dari koneksi jaringan yang telah di rancang, untuk skema rancangan program penelitian dapat dilihat pada gambar dibawah ini :

Gambar 3.3 Skema Rancangan Program Penelitian

3.4.2 Skema Rancangan Alur Pengujian Koneksi Jaringan pada *Cisco Router*

Prosedur penelitian kedua yaitu Skema Rancangan Alur Pengujian Koneksi Jaringan pada *Cisco Router* hampir sama dengan rancangan program penelitian tapi hanya berbeda pada fokus pengujian koneksi jaringan meliputi Perancangan Topologi Jaringan, Konfigurasi Jaringan, Pada PC Laptop Uji Coba Jaringan akan melihat status koneksi jaringan , Pc *Client* untuk uji coba data *download* pada jaringan, yang mana dapat dilihat pada gambar dibawah ini :

Gambar 3.4 Skema Rancangan Pengujian Koneksi Jaringan

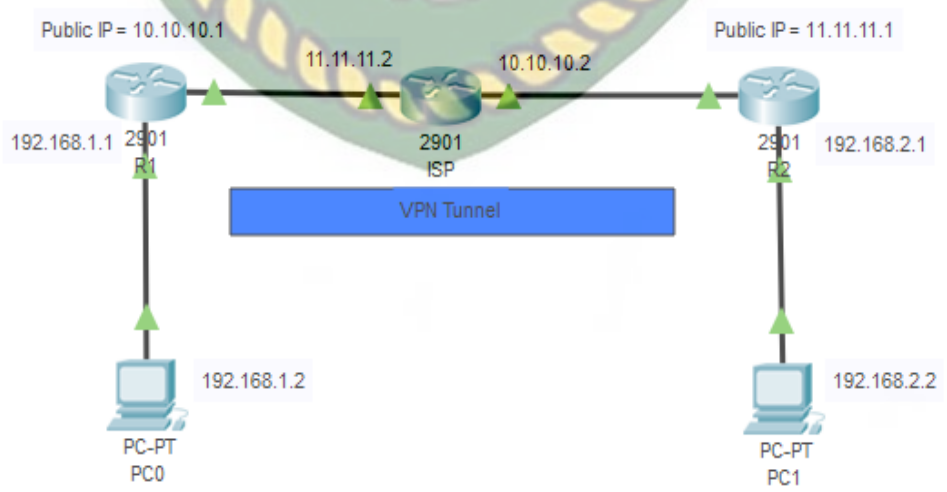
BAB IV

HASIL DAN PEMBAHASAN

Dalam penelitian yang sudah dilakukan menggunakan router cisco didalam suatu jaringan yang sudah diimplementasi VPN yang menggunakan protocol L2TP/IPSEC, dengan melakukan pengiriman paket kejaringan untuk mengetahui tingkat keamanan dari segi enkripsi data dari jaringan tersebut, Dan menguji hasil pengiriman data yang sampai pada tujuan. Maka adapun tahap dalam implementasinya adalah sebagai berikut :

4.1 Perancangan

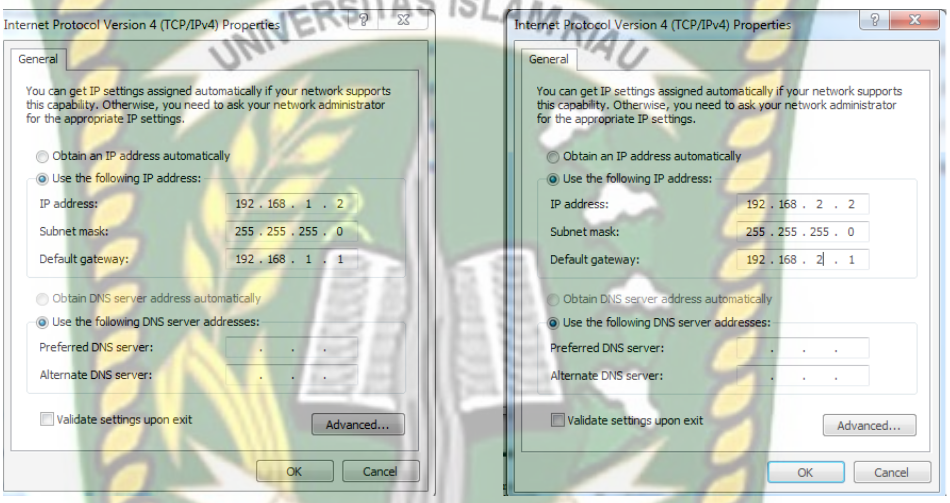
Pada tahap ini dilakukan pengembangan arsitektur jaringan yang telah ada pada jaringan sebelumnya untuk menambahkan sebuah router cisco sebagai router VPN *server* dan *client*. Pengembangan arsitektur jaringan yang akan diterapkan pada jaringan ini dijelaskan pada gambar dibawah ini.



Gambar 4.1 Skema Jaringan Usulan

4.2 *Setting Ip Address*

Sebelum melakukan pengaturan-pengaturan lain seperti *setting ip router*, dan sebagainya, terlebih dahulu mengatur *ip address* pada setiap komputer. Yang berguna sebagai identitas yang mudah dikenali untuk setiap *interface* yang terhubung.



Gambar 4.2 *Setting IP Address*

Ip address 192.168.1.2 digunakan untuk komputer 1 (server) dengan *subnet mask* 255.255.255.0 dan *gateway* 192.168.1.1 dan *Ip address* 192.168.2.2 digunakan untuk komputer 2 (client) dengan *subnet mask* 255.255.255.0 dan *gateway* 192.168.2.1 .

4.3 Konfigurasi *Router*

a. Setting *ip address* untuk masing-masing *router*

Kode program 1

```
Router > enable
Router # configure terminal
Router (config) # hostname R1
```

Kode program 1 merupakan perintah untuk mengaktifkan router, memasuki terminal router dan mengganti nama router, router pertama diberi dengan nama R1.

Kode Program 2

```
R1 (config) # int g0/1
R1 (config-if) # ip address 192.168.1.1 255.255.255.0
R1 (config-if) # no shutdown
R1 (config-if) # int g0/0
R1 (config-if) # ip address 10.10.10.1 255.255.255.0
R1 (config-if) # no shutdown
R1 (config-if) # exit
R2 (config) # ip route 0.0.0.0 0.0.0.0 10.10.10.2
```

Kode program 2 merupakan perintah untuk menambahkan *ip address* 192.168.1.1 ke *router* di slot *interface* g0/1 dan ip public 10.10.10.1 di slot g0/0, perintah *no shutdown* berfungsi untuk mengaktifkan slot *int* g0/1 dan g0/0 *dirouter* dan untuk perintah *ip route* berfungsi untuk membuat *routing* antara beberapa *route*r.

Kode Program 3

```
Router > enable
Router # configure terminal
Router (config) # hostname R2
```

Kode program 3 merupakan perintah untuk mengaktifkan router, memasuki terminal router dan mengganti nama router, router kedua diberi dengan nama R2.

Kode Program 4

```
R2 (config) # int g0/1
R2 (config-if) # ip address 192.168.1.1 255.255.255.0
R2 (config-if) # no shutdown
R2 (config-if) # int g0/0
R2 (config-if) # ip address 10.10.10.1 255.255.255.0
R2 (config-if) # no shutdown
R2 (config-if) # exit
R2 (config) # ip route 0.0.0.0 0.0.0.0 11.11.11.2
```

Kode program 4 merupakan perintah untuk menambahkan *ip address* 192.168.2.1 ke router di slot *interface* g0/1 dan ip public 11.11.11.1 di slot g0/0, perintah *no shutdown* berfungsi untuk mengaktifkan slot int g0/1 dan g0/0 dirouter dan untuk perintah *Ip route* berfungsi untuk membuat *routing* antara beberapa *router*.

Kode Program 5

```
Router > enable
Router # configure terminal
Router (config) # hostname ISP
```

Kode program 5 merupakan perintah untuk mengaktifkan router, memasuki terminal router dan mengganti nama router, router ketiga diberi dengan nama ISP.

Kode Program 6

```
ISP (config) # int g0/0
ISP (config-if) # ip address 10.10.10.2 255.255.255.0
ISP (config-if) # no shutdown
ISP (config-if) # int g0/1
ISP (config-if) # ip address 11.11.11.2 255.255.255.0
ISP (config-if) # no shutdown
ISP (config-if) # exit
ISP (config) # ip route 192.168.1.0 255.255.255.0 10.10.10.1
ISP (config) # ip route 192.168.2.0 255.255.255.0 11.11.11.1
```

Kode program 6 merupakan perintah untuk menambahkan *ip address* 10.10.10.2 ke router di slot *interface* g0/1 dan 11.11.11.2 di g0/0, perintah *no shutdown* berfungsi untuk mengaktifkan slot int g0/1 dan g0/0 dirouter dan untuk perintah *Ip route* berfungsi untuk membuat *routing* antara beberapa *router* dan ip address routingnya 192.168.1.0 dan 192.168.2.0 .

b. Aktifkan vpdn untuk router pertama dan kedua

Kode Program 7

```
R1 (config) # vpdn enable
R1 (config) # vpdn-group l2tp-group
R1 (config-vpdn) # accept-dialin
```

Pada gambar 4.6 adalah perintah untuk mengaktifkan vpdn yang akan digunakan oleh protocol l2tp.

Kode Program 8

```
R1 (config-vpdn-acc-in) # protocol l2tp
R1 (config- vpdn-acc-in) # virtual-template 1
R1 (config- vpdn-acc-in) # exit
```

Kode program 8 merupakan perintah membuat ip virtual yang ditujukan agar sirouter bisa saling terhubung.

Kode Program 9

```
R1 (config) # vpdn-group l2tp-group
R1 (config-vpdn) # l2tp security crypto-profile ipsec1
R1 (config-vpdn) # exit
```

Kode program 9 merupakan perintah menggunaka vpdn dan l2tp, perintah l2tp security berfungsi untuk menggunakan keamanan yang digunakan untuk ipsec.

c. Konfigurasi *tunneling* untuk R1 dan R2

Kode Program 10

```
R1 (config) # crypto isakmp enable
R1 (config-) # crypto isakmp policy 20
R1 (config-isakmp) # authentication pre share
```

Kode program 10 merupakan perintah untuk mengaktifkan protocol isakmp, isakmp adalah protocol yang digunakan untuk membentuk asosiasi keamanan dan kunci kriptografi. perintah *crypto isakmp policy 20* berfungsi untuk

konfigurasi dengan vpn dimana policy 20 adalah prioritasnya dan untuk perintah *authentication* berfungsi untuk menggunakan pre-share key, dimana kedua kunci harus sama antara R1 ke R2.

Kode Program 11

```
R1 (config-isakmp) # encryption 3des
R1 (config-isakmp) # hash md5
R1 (config-isakmp) # group 1
R1 (config-isakmp) # lifetime 3600
R1 (config-isakmp) # exit
```

Kode program 11 merupakan perintah untuk mengenkripsi, perintah *encryption 3des* berfungsi untuk menggunakan enkripsi tipe *triple DES* sebagai *symmetric cryptography*, perintah *hash md5* berfungsi untuk menggunakan enkripsi algoritma md5, perintah group 1 untuk pertukaran kunci, digunakan diffie helman di group 1, *lifetime 3600* berfungsi untuk meningkatkan kecepatan transfer.

Kode Program 12

```
R1 (config) # crypto isakmp cisco123 address 11.11.11.1
R1 (config) # crypto ipsec transform-set myset esp-3des esp-md5-hmac
```

Kode program 12 merupakan perintah untuk koneksi, perintah *crypto isakmp cisco123* untuk memberikan nama kunci, dalam hal ini cisco123 untuk koneksi router pertama menuju ke router kedua yang menggunakan ip public 11.11.11.1, perintah *crypto ipsec transform-set* berfungsi untuk *setting ipsec* dengan nama myset dan protocol yang digunakan adalah *3des* dan *md5*.

Kode Program 13

```
R2 (config) # crypto isakmp cisco123 address 10.10.10.1
R2 (config) # crypto ipsec transform-set myset esp-3des esp-md5-hmac
```

Kode program 13 merupakan perintah untuk koneksi, perintah *crypto isakmp cisco123* untuk memberikan nama kunci, dalam hal ini cisco123 untuk koneksi router kedua menuju ke router pertama yang menggunakan ip public 10.10.10.1, perintah *crypto ipsec transform-set* berfungsi untuk *setting ipsec* dengan nama myset dan protocol yang digunakan adalah *3des* dan *md5*.

Kode Program 14

```
R1 (cfg-crypto-trans) # access-list 100 permit ip 192.168.1.0 0.0.0.255
                        192.168.2.0 0.0.0.255
R1 (config) # crypto ipsec transform-set myset esp-3des esp-md5-hmac
```

Kode program 14 merupakan perintah memberikan *acess-list* agar jaringan *router* pertama (R1) dan *router* kedua (R2) bisa saling interkoneksi.

Kode Program 15

```
R2 (cfg-crypto-trans) # access-list 100 permit ip 192.168.2.0 0.0.0.255
                        192.168.1.0 0.0.0.255
R1 (config) # crypto ipsec transform-set myset esp-3des esp-md5-hmac
```

Kode program 15 merupakan perintah memberikan *acess-list* agar jaringan *router* kedua (R2) dan *router* pertama (R1) bisa saling interkoneksi.

Kode Program 16

```
R1 (config) # crypto map mymap 20 ipsec-isakmp
R1 (config-crypto-map) # set peer 11.11.11.1
```

Kode program 16 merupakan perintah untuk *setting crypto* mapnya dengan nama mymap dengan nomor urut 20, dan perintah *set peer* berfungsi untuk set koneksi kejaringan 11.11.11.1 (*router* kedua).

Kode Program 17

```
R2 (config) # crypto map mymap 20 ipsec-isakmp
R2 (config-crypto-map) # set peer 10.10.10.1
```

Kode program 17 merupakan perintah untuk *setting crypto* mapnya dengan nama mymap dengan nomor urut 20, dan perintah s*et peer* berfungsi untuk set koneksi kejaringan 10.10.10.1 (*router* pertama).

Kode Program 18

```
R1 (config-crypto-map) # set transform-set myset
R1 (config-crypto-map) # match address 100
R1 (config-crypto-map) # exit
```

Kode program 18 merupakan perintah untuk settingan address *router* pertama dan kedua.

Kode Program 19

```
R1 (config) # int g0/0
R1 (config-if # crypto map mymap
R1 (config-if) #
```

Kode program 19 merupakan perintah untuk memberikan crypto map dislot interface g0/0.

4.4 Pengujian Jaringan

Pada sub-bab ini akan dijelaskan perbedaan yang ditemukan antara jaringan awal sebelum memakai L2TP/IPsec dan jaringan akhir setelah memakai L2TP/IPsec berdasarkan simulasi yang dilakukan oleh penulis.

Akan dilakukan beberapa tahap pengujian yaitu *packetloss* dengan menggunakan perintah '*ping'* pada *command prompt*.

4.4.1 Pengujian Jaringan Awal

Pada pengujian jaringan awal akan dilakukan tes terhadap jaringan yang sedang berjalan tanpa VPN.

1. Packet Loss Test

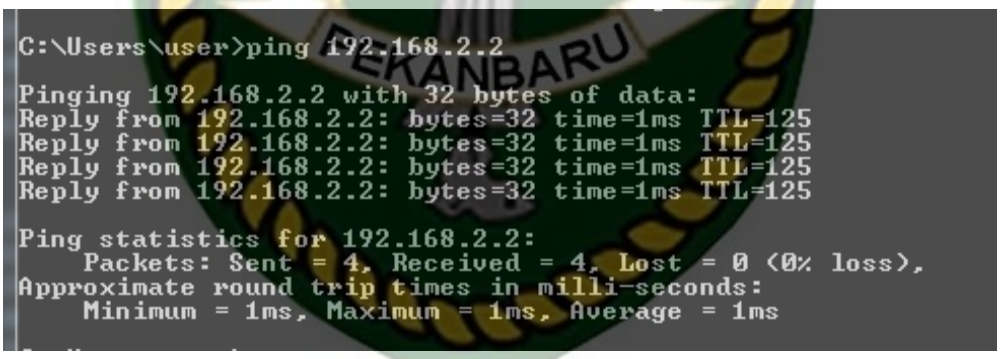
Pengujian packet *loss* dilakukan beberapa kali tes dengan perintah *'ping'* ke *IP* tujuan menggunakan *command prompt* untuk melihat stabilitas koneksi di jaringan tanpa menggunakan VPN. Dan didapatkan hasil sebagai berikut:

Gambar 4.3 Pengujian Konektifitas *Router*

Pada gambar 4.3 hasil dari konektifitas komputer yang sudah terhubung atau berhasil dari masing-masing komputer yang menuju *router* R1 dan R2 dengan menggunakan fasilitas *ping*, ip address 192.168.1.1

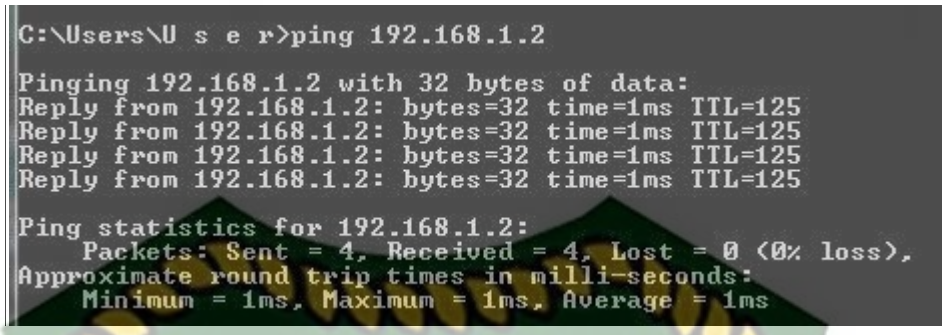
Tabel 4.1 Analisa Pengujian konektifitas Router

No	Skenario Pengujian	Hasil yang diharapkan	Hasil pengujian
1	Ping dari komputer server kerouter pertama	Terhubung	Koneksi berhasil, ip address saling terhubung
2	Ping dari router pertama menuju router kedua dan sebaliknya	Tidak terhubung	Belum dibuat routing antar routernya
3	Ping dari router pertama dan kedua menuju ke komputer	Terhubung	Koneksi berhasil, ip address saling terhubung
4	Ping dari komputer client kerouter kedua	Terhubung	Koneksi berhasil, ip address saling terhubung



Gambar 4.4 Konektiftas Antara 2 Komputer

Pada gambar 4.4 hasil dari konektifitas yang sudah terhubung atau berhasil dari komputer pertama dengan menggunakan *ip address* 192.168.1.2 menuju ke komputer kedua yang menggunakan *ip address* 192.168.2.2 dengan menggunakan fasilitas *ping*.



Gambar 4.5 Konektiftas Antara 2 Komputer (2)

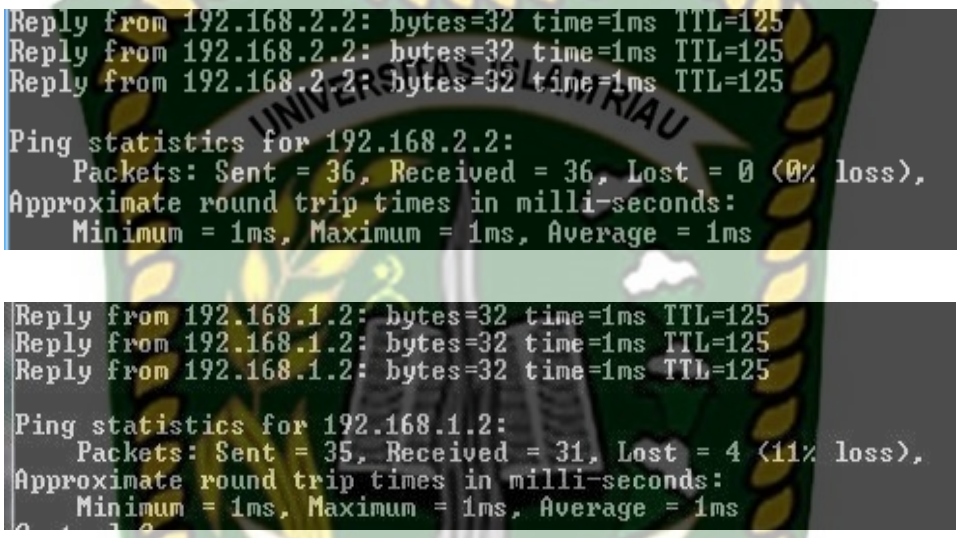
Pada gambar 4.5 hasil dari konektifitas yang sudah terhubung atau berhasil dari komputer pertama dengan menggunakan *ip address* 192.168.2.2 menuju ke komputer kedua yang menggunakan *ip address* 192.168.1.2 dengan menggunakan fasilitas *ping*.

Tabel 4.2 Analisa Pengujian Konektifitas Antara 2 Komputer

No	Skenario Pengujian	Hasil yang diharapkan	Hasil pengujian
1	Ping dari komputer server dan client menuju ke ISP	Terhubung	Koneksi berhasil, ip address saling terhubung dan routing dari router R1 dan R2 menuju ke ISP sudah berhasil
2	Ping dari komputer server ke client dan sebaliknya	Terhubung	Routing antara 3 router sudah terhubung

2. Denial of Service Test

Pengujian ini untuk mengetahui ketahanan koneksi saat dibanjiri paket. Pengujian dilakukan dengan aplikasi *ping*, Setelah dilakukan pengujian didapatkan hasil sebagai berikut:



Gambar 4.6 *DoS Attack* jaringan awal

Pengujian dilakukan dengan mengirimkan 36 paket data didapatkan hasil, bahwa jaringan tidak terputus dan maksimum *round trip* sebesar 1ms dari komputer server menuju komputer client dan maksimum *round trip* sebesar 1ms dari komputer client menuju komputer server dengan mengirim sebanyak 35 paket .

3. Pengiriman paket

```
R1#show crypto ipsec sa

interface: GigabitEthernet0/0
    Crypto map tag: mymap, local addr 10.10.10.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
   current_peer 11.11.11.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.10.10.1, remote crypto endpt.: 11.11.11.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
     current outbound spi: 0x0(0)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
```

Gambar 4.7 Menampilkan Paket

Pada gambar 4.7 *router* pertama (R1) menerima hasil dari dua komputer yang saling mengirim paket satu sama lain dengan menggunakan fasilitas *ping* dirouter, pengirimannya belum melewati *tunnel* atau belum menggunakan vpn.

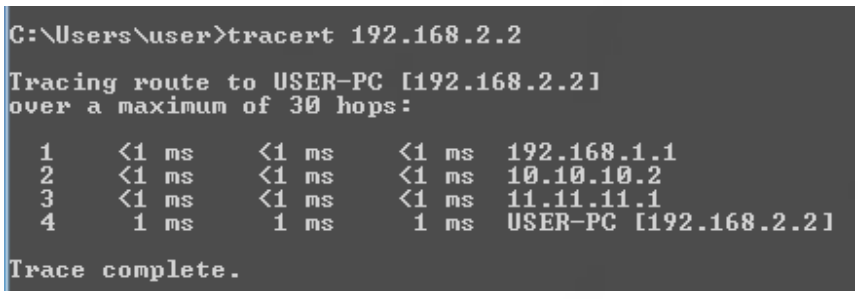
```
R2#show crypto ipsec sa

interface: GigabitEthernet0/0
    Crypto map tag: mymap, local addr 11.11.11.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 10.10.10.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 11.11.11.1, remote crypto endpt.: 10.10.10.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
     current outbound spi: 0x0(0)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
```

Gambar 4.8 Menampilkan Paket (2)

Pada gambar 4.8 *router* kedua (R2) menerima hasil dari dua komputer yang saling mengirim paket satu sama lain dengan menggunakan fasilitas *ping*,pengirimannya belum melewati *tunnel* atau belum menggunakan *vpn*.

Tabel 4.3 Analisa Pengiriman Paket

No	Skenario Pengujian	Hasil yang diharapkan	Hasil pengujian
1	Pengiriman paket dari server keclient menggunakan tunnel	Berhasil	Paket berhasil dikirim ketujuan melewati tunnel tapi vpn belum diaktifkan sehingga paket tidak menggunakan vpn
2	Paket dikirim sebanyak tujuh paket menuju keclient	Berhasil	Paket diterima oleh router client sebanyak nol paket, karena paket belum menggunakan vpn dan enkripsi makanya jumlah paket bernilai nol



Gambar 4.9 tunneling

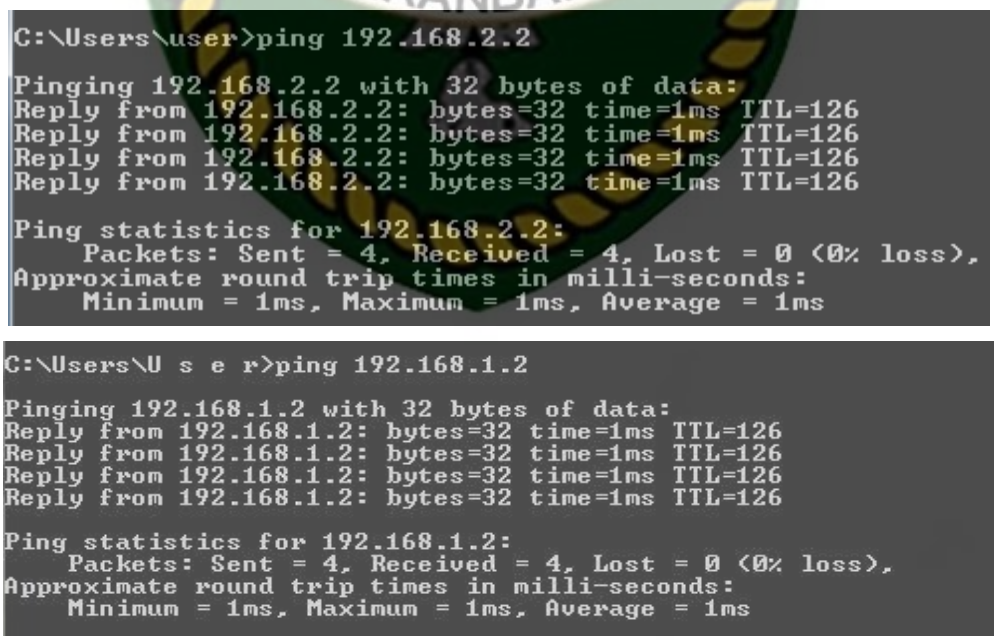
Gambar 4.9 adalah hasil dari pembuatan routing yang nantinya akan dijadikan tunnel yang akan dilewati oleh vpn.

4.4.2 Pengujian Jaringan Akhir

Pada pengujian jaringan akhir ini akan dilakukan beberapa tes seperti yang sudah dilakukan di pengujian jaringan awal tadi. Dengan begitu nanti akan bisa dilihat perbedaan dari kedua jaringan ini antara yang menggunakan VPN dan yang tidak menggunakannya.

1. Packet Loss Test

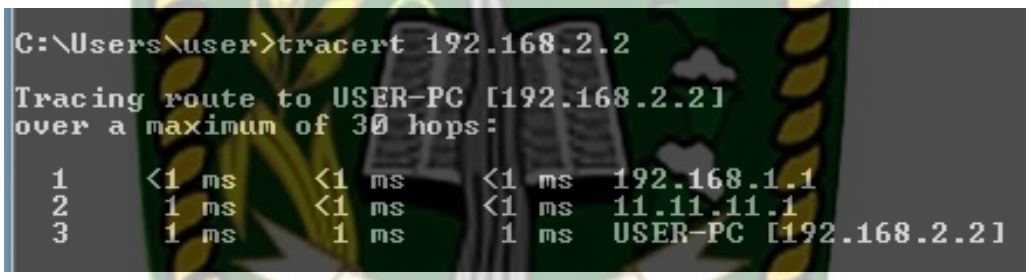
Pengujian *packet loss* dilakukan beberapa kali tes dengan perintah *'ping'* ke *IP* tujuan menggunakan *command prompt* untuk melihat stabilitas koneksi di jaringan menggunakan L2TP/IPSec VPN. Dan didapatkan hasil sebagai berikut:



Gambar 4.10 *Packet Loss* Jaringan VPN

Dari data diatas dapat kita lihat untuk data max dan *average round trip* suatu paket masih dalam nilai yang wajar. Dari percobaan 4 kiriman paket, max round trip = 1ms dan average round trip = 1ms untuk komputer server, dan untuk komputer client max round trip = 1ms dan average round trip = 1ms.

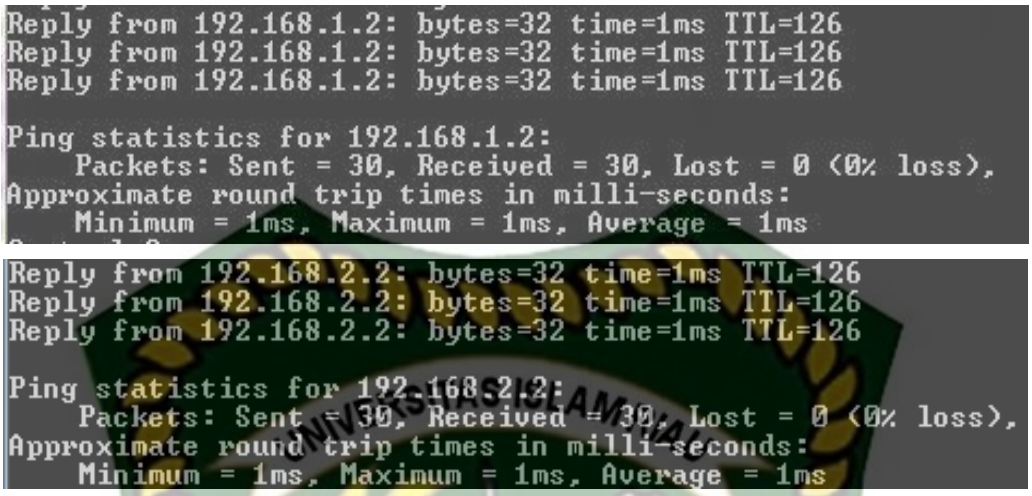
Penulis juga melakukan *trace route* untuk melihat apakah paket yang dikirim sudah melewati (tunnel) jaringan L2TP/IPSEC yang dibuat. Dan seperti gambar dibawah, hasilnya adalah paket dikirim melalui komputer *server* IP 192.168.1.2 dan diteruskan ke IP VPN komputer *client* 192.168.1.2.



Gambar 4.11. *Trace Route* VPN

2. Denial of Service Test

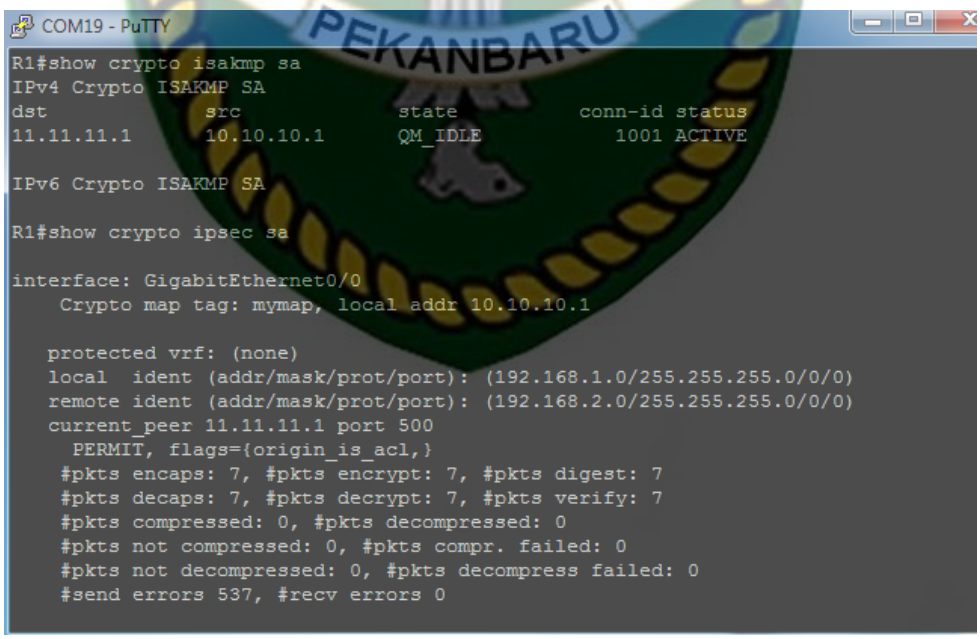
Pengujian ini untuk mengetahui ketahanan koneksi saat dibanjiri paket. Pengujian dilakukan dengan fasilitas *ping*. Setelah dilakukan pengujian didapatkan hasil sebagai berikut:



Gambar 4.12 *Pingflood* Jaringan VPN

Data diatas adalah hasil dari pengujian dengan membanjiri VPN *server* dan client dengan 30 paket data. Hasilnya menunjukan bahwa tidak terjadi kendala atau pun *timeout*.

3. Pengiriman paket



Gambar 4.13 Menampilkan Paket (3)

Pada gambar 4.13 *router* pertama (R1) menerima hasil dari dua komputer yang saling mengirim paket satu sama lain dengan menggunakan fasilitas *ping*, pengirimannya sudah melewati *tunnel* atau sudah menggunakan vpn, paket yang sudah dienkripsi berjumlah 7 dari paket yang belum terenkripsi yang jumlahnya hanya 0.

Gambar 4.14 Menampilkan Paket (4)

Pada gambar 4.14 *router* kedua (R2) menerima hasil dari dua komputer yang saling mengirim paket satu sama lain dengan menggunakan fasilitas *ping*, pengirimannya sudah melewati *tunnel* atau sudah menggunakan vpn, paket yang sudah dienkripsi berjumlah 7 dari paket yang belum terenkripsi yang jumlahnya hanya 0.

Tabel 4.4 Analisa Pengiriman Paket L2tp/Ipsec

No	Skenario Pengujian	Hasil yang diharapkan	Hasil pengujian
1	Pengiriman paket dari server keclient melewati tunnel vpn dan pengiriman client keserver	Berhasil	Paket berhasil dikirim ketujuan melewati tunnel dan menggunakan vpn sehingga paket sudah berhasil diimplementasi l2tp/ipsec
2	Paket dikirim sebanyak tujuh paket menuju keclient dan sebaliknya	Berhasil	Paket diterima oleh router client sebanyak 7 paket dimana paket sudah dienkripsi, dan sudah di deskripsi dan hasil jumlah paketnya tetap sama antara client dan server

BAB V

PENUTUP

5.1 Kesimpulan

Adapun kesimpulan dari proses penelitian menggunakan protocol VPN L2TP/IPsec yang dapat dari penelitian ini adalah :

1. Konsep VPN terbagi atas dua macam koneksi, yaitu *site-to-site* VPN dan *remote access* VPN.
2. Dengan menggunakan L2TP/IPSec maka data yang dikirim ataupun diterima dalam kondisi aman dan sudah dienkripsi dengan baik dan akan dikirim melalui *tunnel*. Sehingga pihak-pihak yang tidak berhak mengakses tidak bisa melihat dan mengakses data tersebut. Karena L2TP/IPSec memberikan layanan keamanan yang sangat baik diantara layanannya yaitu *data integrity*, *confidentiality*, *authentication*, dan *anti replay*.

5.2. Saran-saran

Setelah penelitian yang dilakukan, didapat bahwa teknologi VPN sangat membantu untuk keamanan dan kemudahan akses data dari luar kantor. Untuk itu ada beberapa saran dari penulis untuk kedepannya

1. Untuk keamanan yang lebih baik lagi, ada bagusnya untuk kedepannya bisa ditambahkan autentikasi dengan metode *Port Knocking* yang bisa digunakan pada VPN dengan *router* mikrotik.
2. Agar kedepannya dapat diteliti pada kondisi Internet sebenarnya.

DAFTAR PUSTAKA

Abadillah, Sani Nur, 2011, Pembangunan *VPN* dengan Menggunakan *Virtual Private Server* Untuk Menjaga Keamanan *Internet Publik* (Studi Kasus Pada Jaringan Wifi), Bandung: Universitas Komputer Indonesia.

Anjik Sukamaaji dan Rianto. 2008. " Jaringan Komputer : Konsep Dasar Pengembangan Jaringan dan Keamanan Jaringan", Andi Publisher. Yogyakarta.

Bambang Ardiansyah. (2008). Implementasi *IPSec* pada *VPN*. Jurnal Jaringan Kemanan Komputer.

Iwan Nugroho, Bebas Widada, K. (2015). Perbandingan Performansi Jaringan *Virtual Private Network Metode Point To Point Tunneling Protocol* (PPTP) Dengan Metode *Internet Protocol Security*. TIKomSiN, 1–9.

Martiyanto, Andrian Satria, 2011, Desain dan Implementasi *Virtual Private Network* dan *Web Proxy* Untuk Mengakses Sumber Daya Informasi Lokal Dari Jaringan Publik, Semarang.

Nuraini, Romdon. 2009. Analisis Implementasi *Virtual Private Network* berbasis *L2TP/IPSec*, Bandung, IT Telkom

Purbo, Onno W., 2001, Keamanan Jaringan Internet, Jakarta: Elex Media Komputindo.

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

Sarman, 2006, Server *VPN* berbasis *Linux* dengan *Client.* SMIT. Yogyakarta

Sofana, Iwan, 2004. CISCO CCNA & Jaringan Komputer, 305-32, Bandung.

Winarno, Sugeng, 2006. Jaringan Komputer dengan TCP/IP, Informatika, Bandung.

Sunyoto, Wendy, Aris, (2006), VPN Sebuah Konsep Teori dan Implementasi, Buku Web Networking : Surabaya.