

## BAB IV

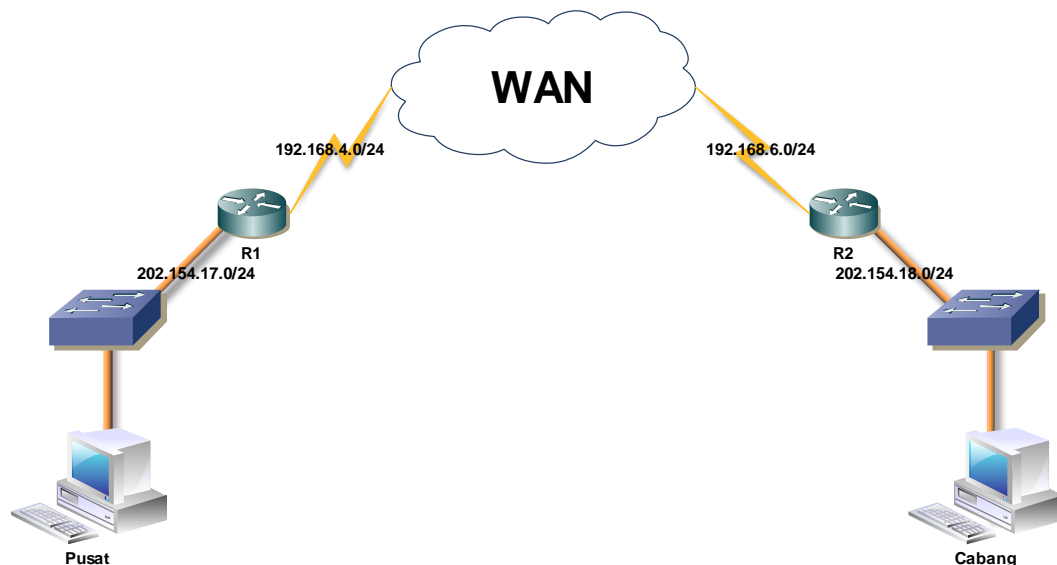
### IPSEC PADA ROUTER CISCO 1841

Pada bab ini akan dibahas secara terperinci tentang Virtual Private Network dengan menggunakan protokol IPsec pada Router Cisco 1841, berdasarkan proses analisa yang sudah dilakukan sebelumnya. Adapun pada bab ini, akan dibagi menjadi beberapa sub-bab, yakni skenario uji coba, tolok ukur, metode penelitian, uji coba dan analisa, serta hasil analisa. Selain itu juga terdapat sebuah sub-bab tentang aplikasi Cisco Configuration Professional yang berguna untuk mempermudah konfigurasi Router Cisco 1841.

Pada bab ini akan dibahas beberapa analisa, antara lain analisa biaya, analisa keamanan, serta analisa mengenai hubungan antara metode autentikasi, enkripsi, hash, serta jumlah router pada WAN terhadap performa atau kinerja dari VPN IPsec.

Tujuan dari analisa ini adalah untuk mencari sebuah metode enkripsi VPN, yang aman dan efisien untuk diaplikasikan pada sebuah sistem yang nyata.

#### 4.1. Skenario Uji Coba



**Gambar 4.1**  
**Skenario Uji Coba**

Untuk melakukan analisa terhadap keamanan dan kinerja dari VPN ini, diperlukan sebuah skenario untuk mempermudah proses analisa. Seperti digambarkan pada gambar 4.1, terdapat beberapa komponen yang diperlukan pada skenario ini.

Terdapat dua buah Router Cisco 1841 yang berfungsi sebagai gateway VPN pada masing-masing ujung tunnel VPN. Masing-masing ujung, dalam hal ini gateway VPN, terhubung dengan sebuah komputer client, yang nantinya akan berkomunikasi melalui tunnel VPN yang terbentuk.

Dalam analisa yang dilakukan pada bab ini, akan diperbandingkan beberapa kombinasi dari metode enkripsidan hash yang disediakan oleh framework IPSec yang dimiliki oleh Router Cisco 1841 dengan sistem operasi “c1841-advsecurityk9-mz.124-23.bin”. Berikut ini metode-metode enkripsi dan hash yang akan digunakan oleh dalam studi analisa ini:

**Tabel 4.1**  
**Metode-Metode IPsec Yang Akan Digunakan**

<b>Autentikasi</b>	Pre-shared Key	PSK
	Rivest Shamir Adleman Encryption	RSA-Encr
	Rivest Shamir Adleman Signature	RSA-Sig
<b>Enkripsi</b>	Data Encryption Standard	DES
	Key triple DES	3DES
	Advanced Encryption Standard	AES
<b>Hash</b>	Secure Hash Standard	SHA
	Message Digest 5	MD5

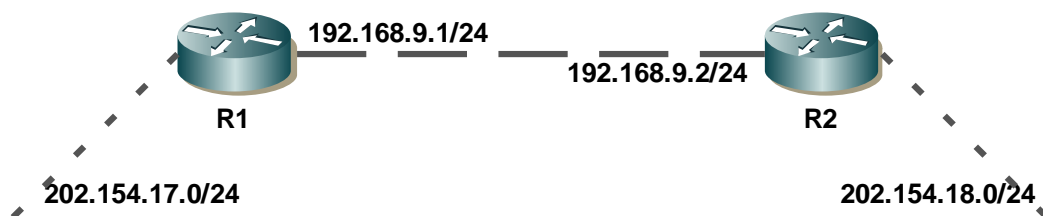
Dalam studi analisa ini, pembentukan jaringan VPN akan dikombinasikan antara metode enkripsi, dan hash yang tersedia. Autentikasi, hanya digunakan pada saat awal pembentukan VPN saja, atau pada saat pembentukan Inketnet Key Exchange (IKE), tetapi tidak digunakan lagi saat proses komunikasi berlangsung. Selain itu, implementasi dari metode autentikasi RSA, baik RSA Encryption maupun RSA Signature, membutuhkan *digital certificate* resmi dari badan sertifikasi keamanan seperti Verizon dan Cybertrust. Oleh karena itu, metode autentikasi yang digunakan pada uji coba ini adalah metode Pre-shared Key, dengan key “cisco”. Sedangkan untuk algoritma Diffie-Hellman, digunakan algoritma Diffie-Hellman dengan group tertinggi, yakni DH5. Konfigurasi router

untuk masing-masing kombinasi akan dibahas pada sub-bab berikutnya, sesuai dengan kombinasi yang digunakan.

Selain metode-metode autentikasi, enkripsi, serta hash, pada studi analisa ini juga dilakukan pengamatan terhadap jumlah router yang dilalui pada WAN, atau setelah keluar dari gateway VPN. Dalam uji coba ini, digunakan tiga buah skenario WAN untuk menguji performa dari koneksi VPN yang dibentuk oleh kedua gateway VPN. Adapun tiga buah skenario tersebut yaitu:

- 0 Router

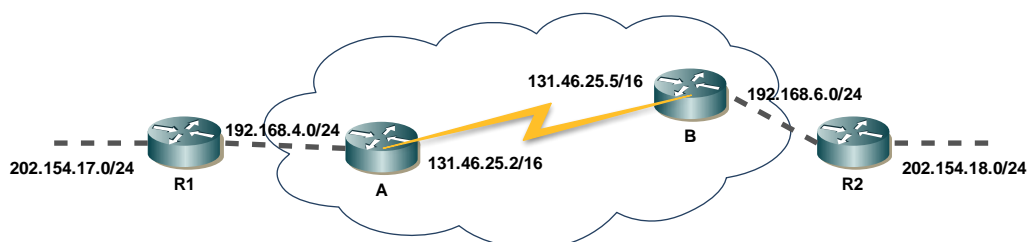
Pada simulasi WAN dengan 0 Router, kedua gateway VPN terhubung secara langsung dengan menggunakan kabel crossover. Dengan demikian jaringan WAN pada skenario ini hanya satu jaringan saja. Gambaran simulasi ini dapat dilihat pada gambar berikut ini.



**Gambar 4.2**  
**Simulasi WAN Tanpa Router**

- 2 Router

Pada simulasi WAN dengan 2 Router, dua buah gateway VPN terhubung melalui dua buah router yang disusun seperti gambar 4.3 berikut.



**Gambar 4.3**  
**Simulasi WAN dengan 2 Router**

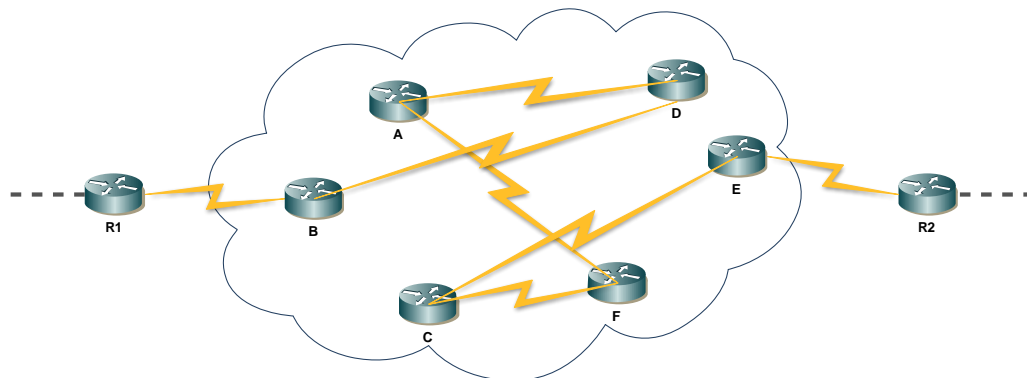
Dengan demikian, jika R1 hendak mengirimkan paket data menuju R2, maka paket tersebut harus melalui Router A dan Router B, dan sebaliknya. Konfigurasi kedua Router yang bertindak sebagai WAN tersebut, dapat dilihat pada tabel berikut ini:

**Tabel 4.2**  
**Konfigurasi Router A dan B pada WAN 2 Router**

Router	Interface	IP Address	Subnet Mask
A	Serial 0	131.46.25.2	255.255.0.0
	Fast Ethernet 0	192.168.4.1	255.255.255.0
B	Serial 0	131.46.25.5	255.255.0.0
	Fast Ethernet 0	192.168.6.1	255.255.255.0

- **6 Router**

Dalam simulasi WAN dengan 6 router ini, jaringan WAN akan disimulasikan dengan menggunakan menggunakan enam buah Router yang dihubungkan satu sama lain seperti tampak pada gambar 4.4.



**Gambar 4.4**  
**Simulasi WAN**

Keenam router tersebut dihubungkan satu sama lain dengan protokol routing RIP. Sehingga untuk mengirimkan paket data dari R1 menuju R2 harus melalui jalur B-D-A-F-C-E. Adapun konfigurasi umum dari keenam router tersebut adalah sebagai berikut:

- **Router A**

Interface Serial 0:

IP Address : 110.23.52.1/8

Bandwidth : 128,000

Clock Rate : 64,000

Interface Serial 1:

IP Address : 65.38.14.1/8

Bandwidth : 128,000

Clock Rate : -

• **Router B**

Interface Serial 0:

IP Address : 131.46.25.2/16

Bandwidth : 128,000

Clock Rate : 64,000

Interface Serial 1:

IP Address : 124.35.147.2/8

Bandwidth : 128,000

Clock Rate : 64,000

Interface Fast Ethernet 0:

IP Address : 192.168.4.1/24

Bandwidth : 128,000

• **Router C**

Interface Serial 0:

IP Address : 148.55.62.3/16

Bandwidth : 128,000

Clock Rate : 64,000

Interface Serial 1:

IP Address : 92.54.35.3/8

Bandwidth : 128,000

Clock Rate : -

- **Router D**

Interface Serial 0:

IP Address : 110.23.52.4/8  
Bandwidth : 128,000  
Clock Rate : -

Interface Serial 1:

IP Address : 124.35.147.4/8  
Bandwidth : 128,000  
Clock Rate : -

- **Router E**

Interface Serial 0:

IP Address : 131.46.25.5/16  
Bandwidth : 128,000  
Clock Rate : -

Interface Serial 1:

IP Address : 92.54.35.5/8  
Bandwidth : 128,000  
Clock Rate : 64,000

Interface Fast Ethernet 0:

IP Address : 192.168.6.1/24  
Bandwidth : 128,000

- **Router F**

Interface Serial 0:

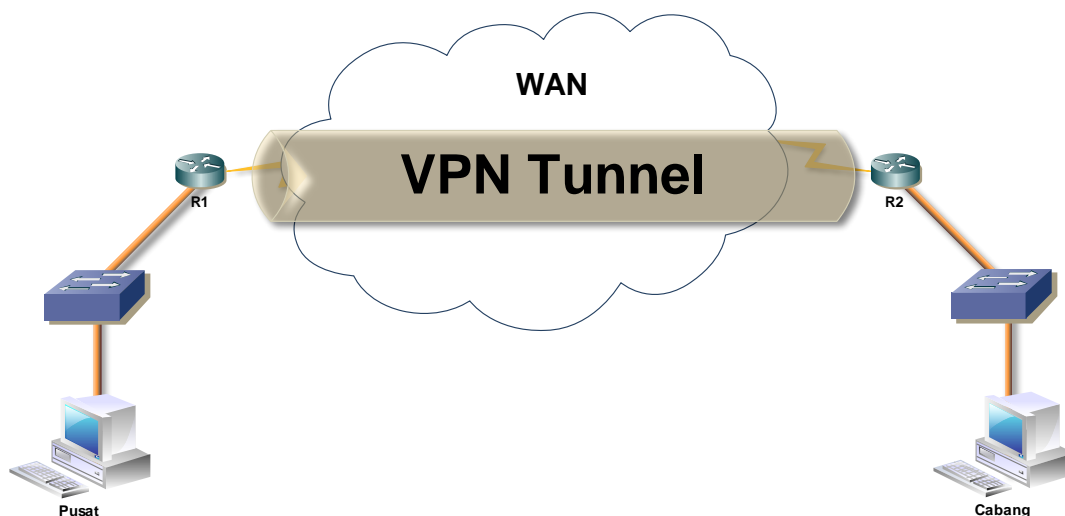
IP Address : 148.55.62.6/16  
Bandwidth : 128,000  
Clock Rate : -

Interface Serial 1:

IP Address : 65.38.14.6/8  
Bandwidth : 128,000  
Clock Rate : 64,000

Terdapat beberapa protokol routing yang disediakan oleh Router Cisco 1841, antara lain Static Routing, RIP, OSPF, IGRP, dan EIGRP. Dalam studi analisa ini, akan digunakan protokol routing RIP versi 1 karena penggunaannya yang cukup sederhana. Protokol routing RIP digunakan baik pada router gateway VPN, maupun router yang bertindak sebagai WAN.

Router R1 terhubung pada jaringan WAN, melalui interface Fast Ethernet 0 Router B. Sedangkan Router R2 terhubung pada Fast Ethernet 0 Router E. Dengan demikian telah terbentuk sebuah jaringan yang menghubungkan jaringan pusat dan jaringan cabang melalui jaringan publik, atau WAN.



**Gambar 4.5**  
**VPN Tunnel**

Jaringan komunikasi yang terbentuk antara kedua sub-jaringan tersebut, masih merupakan jaringan publik yang dikatakan tidak aman. Karena paket yang dikirimkan, tidak mengalami enkripsi sama sekali sejak keluar dari komputer. Oleh karena itu, perlu dibentuk sebuah jaringan VPN yang dapat diibaratkan sebagai sebuah tunnel atau terowongan. Pada area WAN tersebut nantinya akan dipasang sebuah komputer yang berfungsi sebagai penyusup yang dapat mengidentifikasi paket-paket yang sedang melewati area WAN tersebut.

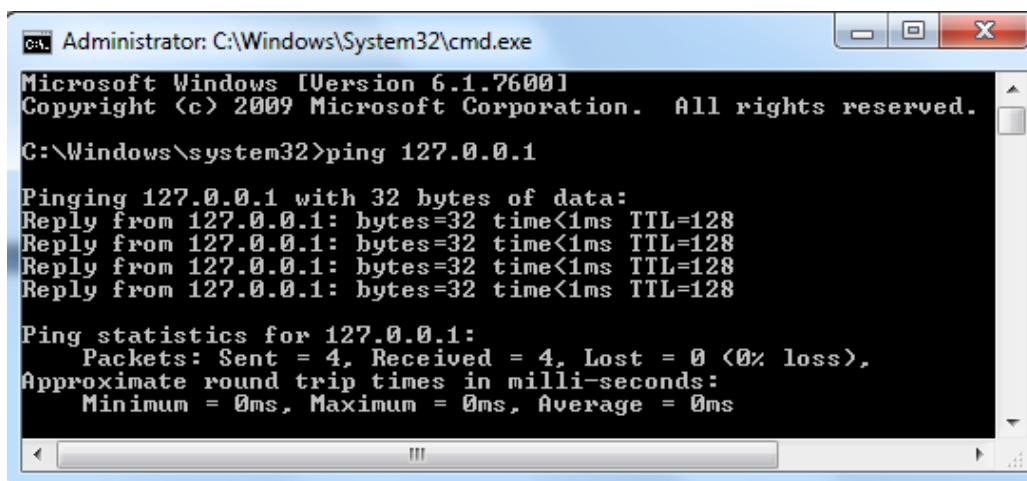
## 4.2. Tolok Ukur

Virtual Private Network memberikan proses enkripsi, autentikasi, dan hash pada paket yang dikirimkan melalui tunnel yang dibuat. Ketiga proses tersebut memerlukan waktu dalam masing-masing prosesnya, baik waktu enkripsi maupun waktu dekripsi. Sehingga untuk membandingkan kombinasi metode-metode yang ada, diperlukan adanya tolak ukur untuk menilai suatu kombinasi.

Terdapat beberapa tolak ukur yang digunakan untuk menilai sebuah kombinasi dari metode-metode enkripsi, dan hash yang ada. Diharapkan dengan tolak ukur yang digunakan, akan diperoleh sebuah kombinasi yang ideal dan efisien. Adapun tolak ukur yang digunakan, berguna untuk menganalisa tingkat kecepatan dan keamanan paket data selama proses pengiriman.

### 4.2.1. PING

PING merupakan sebuah aplikasi umum yang tersedia, baik pada komputer maupun pada router. Dalam operasinya, PING menggunakan protokol ICMP. Tujuan utama PING adalah untuk menguji keterjangkauan sebuah perangkat yang terhubung pada suatu jaringan..



```

Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
  
```

**Gambar 4.6**  
**PING**

Pada kasus ini akan digunakan aplikasi PING yang terdapat pada sistem operasi Windows, karena seorang pengguna tidak mempedulikan kecepatan antara



router atau gateway, melainkan kecepatan antara komputer yang sangat diutamakan.

PING merupakan aplikasi standar Windows. Pada Windows, aplikasi ini dijalankan pada Windows Command Prompt yang terdapat pada menu Accessories. Untuk menjalankan PING pada Command Prompt, masukkan perintah “ping <alamat IP tujuan>”. Apabila koneksi berjalan dengan normal, maka akan ditampilkan pesan yang berisi:

- Reply from  
Balasan dari perangkat tujuan
- Bytes  
Ukuran data yang dikirimkan
- Time  
Waktu yang diperlukan mulai data dikirimkan sampai kembali diterima.
- TTL  
Time to live, adalah waktu yang disematkan dalam paket data yang dikirimkan melalui jaringan untuk menyatakan berapa lama paket tersebut bisa beredar di dalam jaringan.

Terdapat beberapa opsi dalam operasi PING ini. Setiap opsi diwakili dengan sebuah huruf. Untuk menjalankan opsi, tambahkan simbol minus (-) diikuti huruf di belakan perintah PING dasar. Adapun beberapa opsi tambahan yang sering digunakan adalah sebagai berikut:

- -t  
Melakukan PING terus menerus hingga diberhentikan oleh pengguna.
- -n<jumlah>  
Melakukan PING sebanyak jumlah yang diinginkan.
- -i TTL  
Melakukan PING dengan set Time to Live paket yang diinginkan.

- -r<jumlah>

Melakukan PING disertai dengan rute yang dilewati sebanyak jumlah yang diinginkan.

- -s<jumlah>

Melakukan PING disertai pencatatan waktu pada setiap hop yang dilewati sebanyak jumlah yang diinginkan.

Dalam studi analisa ini, akan digunakan nilai *time* rata-rata, dari 4 kali PING. Nilai ini akan dihitung dalam satuan *millisecond*. Semakin rendah nilai *time*, semakin cepat pula koneksi antara dua perangkat yang bersangkutan.

#### 4.2.2. Aplikasi Sederhana

Untuk membantu penelitian keamanan data ini digunakan sebuah program yang dapat mengaplikasikan kegunaan Virtual Private Network pada dunia nyata. Oleh karena itu, untuk keperluan analisa ini, dibuat sebuah program percakapan sederhana, yang berbasis *client server*.

Berbeda dengan PING, program ini berfungsi untuk saling berkiriman pesan antar komputer. Program ini dibuat dengan Visual Basic .NET framework versi 4, melalui Visual Studio 2010. Dengan memanfaatkan socket programming yang terdapat pada library yang telah disediakan dan beberapa library lainnya, program ini dapat mengirimkan data melalui jaringan. Serta sebuah class bernama “client”. Isi dari class ini, disertakan pada halaman lampiran.

##### Listing 4.1 Penggunaan Library Pada Program

```
1 : Imports System.IO
2 : Imports System.Net
3 : Imports System.Net.Sockets
4 : Imports System.Text
5 : Imports System.Threading
```

Program ini berfungsi mengirimkan pesan melalui aliran data TCP, yang disertai dengan timestamp pada sisi klien. Dengan menggunakan port 8080, yang terbuka pada client maupun server.

**Listing 4.2 Proses Pengiriman Pesan Pada Client**

```

1 : Dim jam As String
2 : Dim men As String
3 : Dim det As String
4 : Dim mil As String
5 : jam = Now.Hour.ToString
6 : men = Now.Minute.ToString
7 : det = Now.Second.ToString
8 : mil = Now.Millisecond.ToString
9 : msg = msg + "[" + jam + "," + men + "," + det + "," + mil +
    "]"
10 : Dim bytes() As Byte
11 : bytes = System.Text.Encoding.ASCII.GetBytes(_MESSAGE & msg)
12 : If stream.CanWrite Then
13 :     stream.Write(bytes, 0, bytes.Length)
14 :     stream.Flush()
15 :     Thread.Sleep(100)
16 : End If

```

Pada sisi server, saat pesan diterima program akan menambahkan pesan tersebut dengan timestamp yang menunjukkan waktu penerimaan pesan.

**Listing 4.3 Proses Penerimaan Pesan Pada Server**

```

1 : Dim jam As String
2 : Dim men As String
3 : Dim det As String
4 : Dim mil As String
5 : jam = Now.Hour.ToString
6 : men = Now.Minute.ToString
7 : det = Now.Second.ToString
8 : mil = Now.Millisecond.ToString
9 : msg = msg + "{" + jam + "," + men + "," + det + "," + mil +
    "}"
10 : list_msg.Items.Add(msg)

```

Dengan menggunakan program ini, kedua buah komputer akan berkomunikasi dan nantinya, diharapkan isi dari pesan yang dikirimkan dapat terdeteksi oleh wireshark. Pembahasan tentang wireshark akan dibahas pada sub bab berikutnya.

**4.2.3. Wireshark**

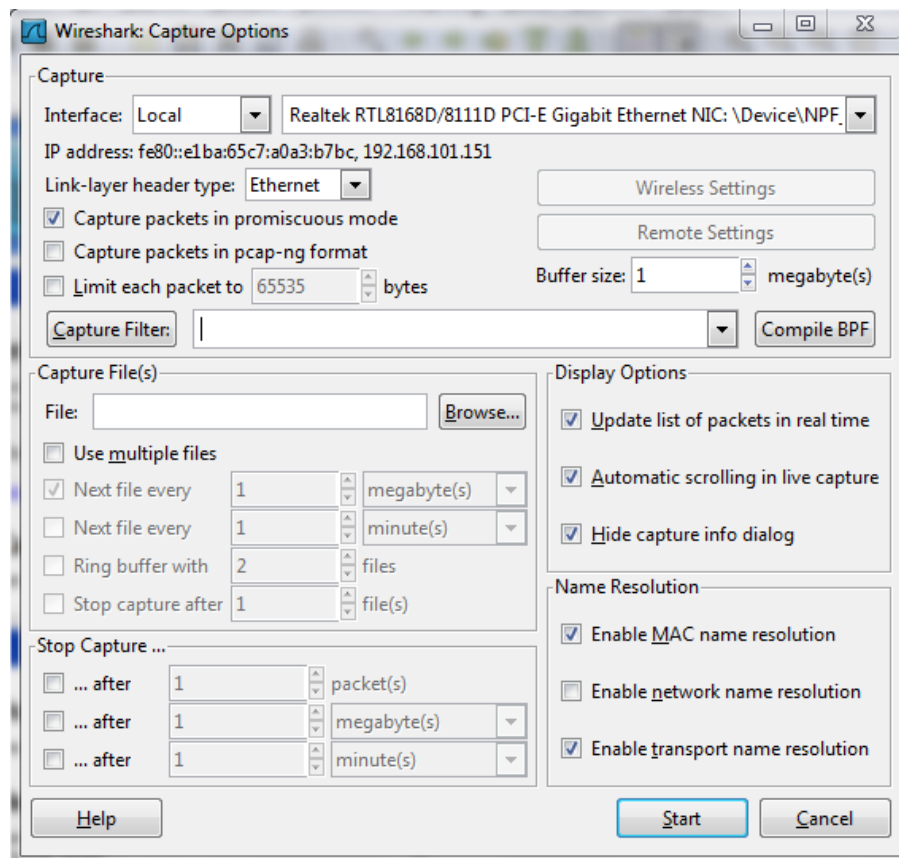
Untuk menguji keamanan saat pengiriman, digunakan sebuah aplikasi bernama Wireshark. Sebelum bernama Wireshark, program ini dikenal dengan nama Ethereal yang berfungsi sama, yaitu menangkap paket yang melewati hub.

Pada hub, Wireshark memanfaatkan sistem broadcast yang dilakukan oleh hub untuk menangkap paket.

Saat ini, dengan adanya teknologi port monitoring, tidak hanya paket yang melewati Hub yang dapat ditangkap oleh Wireshark, paket yang melewati Switch juga dapat ditangkap dan dianalisa oleh Wireshark.

Hub sendiri sudah jarang digunakan, karena kurang efisien dibandingkan dengan switch. Karena sistem kerja hub adalah broadcast yang mengirim paket ke semua peer yang terhubung dengan hub. Sehingga hub bersifat half duplex. Selain itu karena masalah keamanan juga, hub juga ditinggalkan.

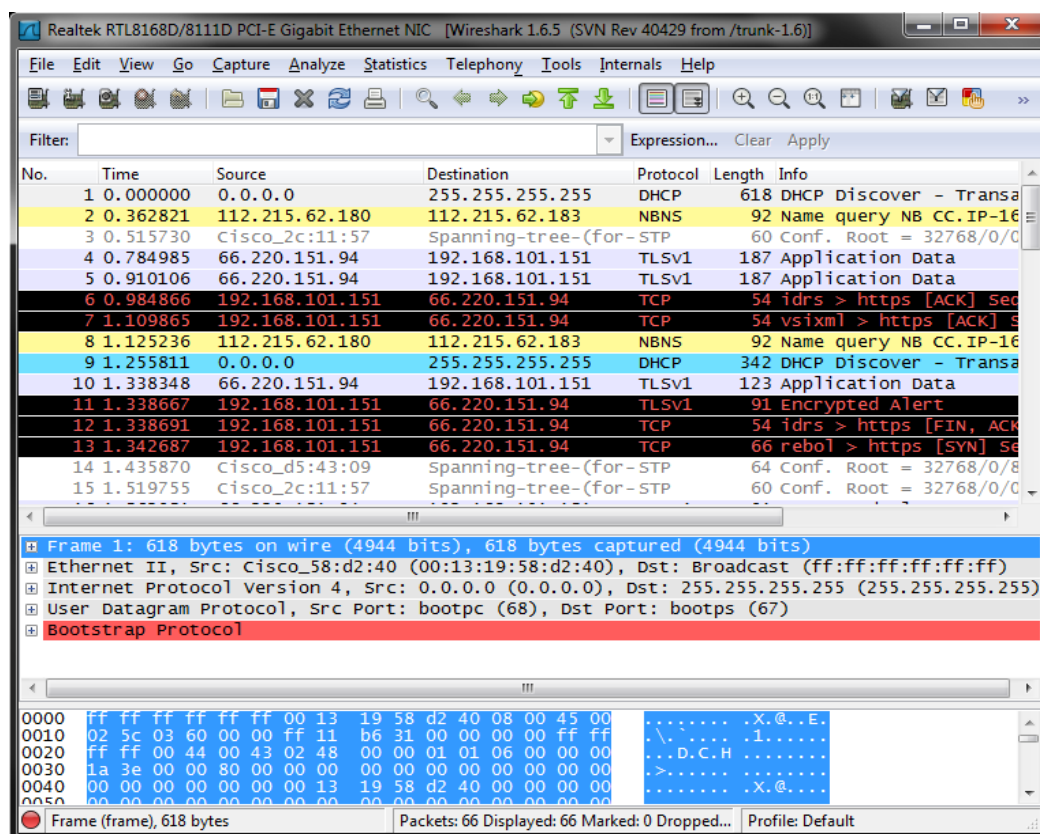
Terdapat tiga buah fasilitas Wireshark yang akan digunakan dalam studi analisa ini, yaitu capture, filter, dan analyze stream. Fungsi capture berfungsi untuk menangkap paket data. Filter berfungsi untuk menyaring paket data. Sedangkan analyze stream berfungsi untuk menganalisa isi paket data.



**Gambar 4.7**  
**Capture Option Wireshark**

Fungsi capture dapat dijalankan dengan memilih menu capture, dan submenu options. Pada window yang terbuka, dapat ditentukan melalui interface mana fungsi capture akan dilakukan. Dan kemudian fungsi capture dapat dimulai dengan menekan tombol start. Pada saat fungsi capture dijalankan, maka akan ditampilkan semua paket data yang melewati hub. Hasil capture dapat dilihat seperti pada gambar 4.8. Warna hasil capture, dibedakan berdasarkan protokol yang digunakan oleh paket yang melintas, sehingga mempermudah dalam mengamati paket yang ada.

Pada studi analisa ini, pilihan-pilihan pada capture option ini akan digunakan pilihan-pilihan standar yang sudah diatur pada saat wireshark dibuka, karena pilihan-pilihan standar sudah mencukupi kebutuhan dari studi analisa ini. Meskipun terdapat beberapa pilihan yang sifatnya lebih terperinci sehingga dapat memanipulasi data yang dihasilkan oleh capture wireshark.



**Gambar 4.8**  
**Capture Wireshark**

Wireshark memiliki fungsi penyaringan atau filter dalam operasinya. Dasar dari filter yang digunakan dapat bermacam-macam. Adapun beberapa filter yang terdapat pada Wireshark antara lain TCP Port, IP Address, UDP Port, dan beberapa filter yang lainnya. Filter ini juga dapat digunakan bertumpuk dengan operasi AND maupun OR. Pada studi analisa ini, digunakan filter yang sesuai dengan socket yang digunakan oleh program, yaitu TCP Port 8080, IP Address 202.154.17.10, dan IP Address 202.154.18.10.

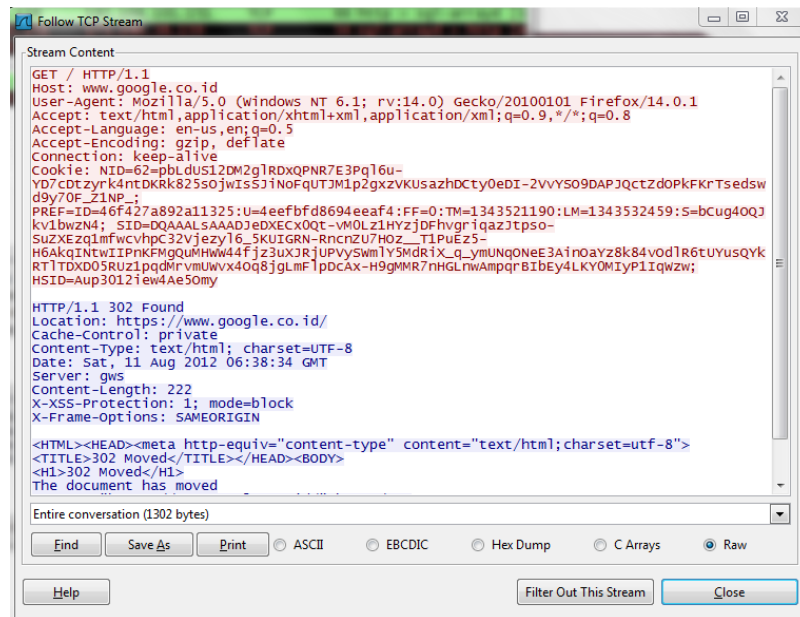
Fungsi filter dijalankan dengan memasukkan ekspresi filter pada textbox yang ada pada window utama Wireshark. Input ekspresi filter dapat dimasukkan melalui window expression, yang menyediakan daftar parameter filter yang ada. Window expression ini dapat dibuka dengan menekan tombol expression yang terletak di samping textbox filter. Filter dapat dimulai dengan menekan tombol apply di samping textbox filter.

Pada saat fungsi filter dijalankan, maka hanya paket data yang memenuhi ekspresi filter saja yang ditampilkan pada Wireshark. Contoh hasil filter dapat dilihat seperti pada gambar di bawah ini.

Filter: tcp.port == 80						
Expression... Clear Apply						
No.	Time	Source	Destination	Protocol	Length	Info
9	2.438980	192.168.101.151	173.194.38.151	TCP	66	5274
11	2.488066	173.194.38.151	192.168.101.151	TCP	66	http
12	2.488118	192.168.101.151	173.194.38.151	TCP	54	5274
13	2.488235	192.168.101.151	173.194.38.151	HTTP	878	GET /
14	2.550920	173.194.38.151	192.168.101.151	TCP	60	http
15	2.565692	173.194.38.151	192.168.101.151	HTTP	532	HTTP/
29	2.769585	192.168.101.151	173.194.38.151	TCP	54	5274

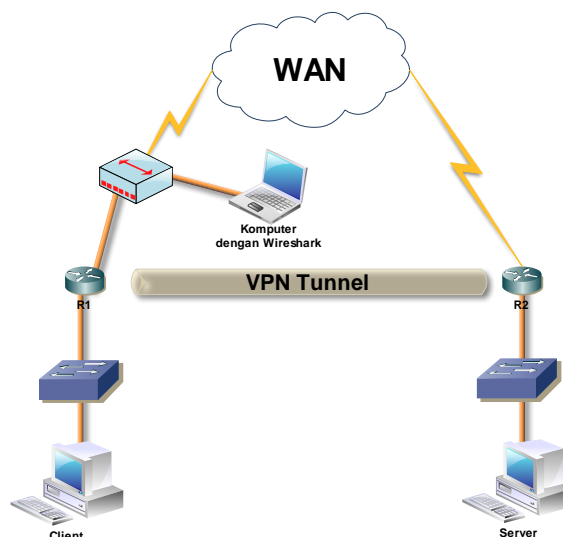
**Gambar 4.9**  
**Filter Wireshark**

Fungsi analyze stream, memungkinkan potongan paket data untuk diamati secara keseluruhan. Wireshark mampu menelusuri dan menyusun potongan paket, meskipun paket yang dianalisa bukan paket awal. Fungsi ini terbatas hanya pada stream TCP, UDP, dan SSL saja. Untuk menjalankan fungsi ini, pilih salah satu potongan paket yang ada, lalu buka menu analyze, dan pilih jenis stream dari paket tersebut.



**Gambar 4.10**  
**Analyze TCP Stream**

Penggunaan Wireshark secara legal antara lain sebagai perangkat pemantau jaringan, di mana lalu lintas jaringan dapat dipantau secara langsung. Sehingga jika terdapat paket yang mencurigakan, pihak yang berwenang dapat bertindak. Selain tindakan legal, Wireshark juga dapat digunakan untuk penggunaan ilegal, seperti menyadap isi pesan yang lewat, bahkan password yang tidak terenkripsi dapat terlihat dengan jelas.



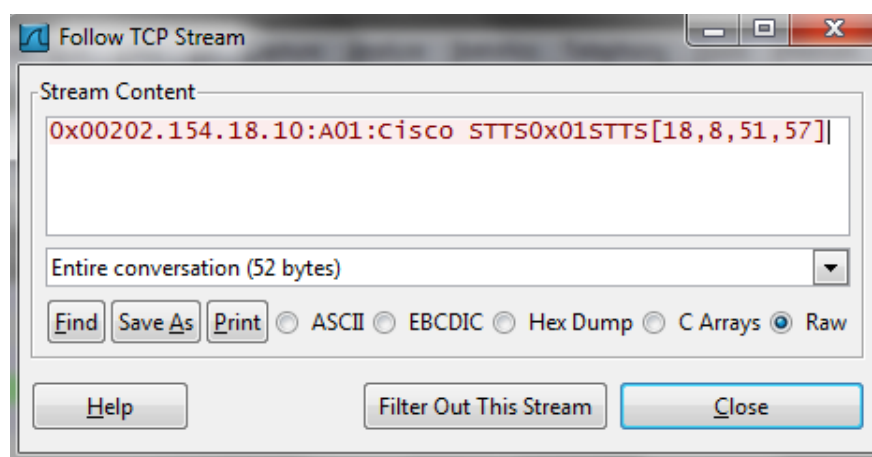
**Gambar 4.11**  
**Posisi Komputer Penangkap Paket Data**

Dalam studi analisa ini, wireshark akan dipasang pada sebuah komputer yang akan terhubung pada sebuah hub yang menghubungkan dua router yang bertindak sebagai gateway VPN. Posisi komputer untuk menangkap paket data tersebut pada studi analisa ini, dapat dilihat pada gambar 4.11.

Filter: tcp.stream eq 15							Expression...	Clear	Apply
No.	Time	Source	Destination	Protocol	Length	Info			
75	60.122116	202.154.17.10	202.154.18.10	TCP	66	danf-ak2 > http-alt [SYN] Seq=0 wi			
76	60.138017	202.154.18.10	202.154.17.10	TCP	66	http-alt > danf-ak2 [SYN, ACK] Seq			
77	60.138273	202.154.17.10	202.154.18.10	TCP	60	danf-ak2 > http-alt [ACK] Seq=1 Ac			
78	60.139766	202.154.17.10	202.154.18.10	HTTP	86	Continuation or non-HTTP traffic			
79	60.370102	202.154.18.10	202.154.17.10	TCP	60	http-alt > danf-ak2 [ACK] Seq=1 Ac			
80	61.206945	202.154.17.10	202.154.18.10	HTTP	74	Continuation or non-HTTP traffic			
81	61.430801	202.154.18.10	202.154.17.10	TCP	60	http-alt > danf-ak2 [ACK] Seq=1 Ac			

**Gambar 4.12**  
**Capture Wireshark Tanpa VPN**

Pada uji coba tanpa VPN dengan menggunakan program yang telah dibahas pada sub bab 4.2.2, yang mengirimkan sebuah pesan berisi teks “STTS”, Wireshark menangkap beberapa paket data yang sedang dikirimkan oleh komputer pengirim melalui filter pada port 8080. Hasil capture tersebut dapat dilihat pada gambar 4.12. Dan setelah dilakukan analisa penelusuran terhadap stream paket tersebut, dapat diketahui isi paket tersebut. Adapun hasil analisa tersebut dapat dilihat pada gambar di bawah ini.



**Gambar 4.13**  
**Analyze TCP Stram Wireshark Tanpa VPN**



Setelah dianalisa, paket tersebut berisi pesan “STTS”, dan alamat IP “202.154.18.10”, yang merupakan alamat IP dari komputer yang dituju.

Dengan demikian, dapat diketahui bahwa jaringan internetwork, khususnya Internet bersifat tidak aman. Sehingga diperlukan adanya sebuah sistem keamanan yang dapat melindungi paket-paket data yang dikirimkan melalui jaringan Internet. Dalam pembahasan ini adalah Virtual Private Network.

Filter: (ip.addr==192.168.6.2)		Expression... Clear Apply				
No.	Time	Source	Destination	Protocol	Length	Info
19	28.243978	192.168.4.2	192.168.6.2	ESP	126	ESP (SPI=0xee294764)
20	28.276374	192.168.6.2	192.168.4.2	ESP	126	ESP (SPI=0xeea0e03f)
21	29.239572	192.168.4.2	192.168.6.2	ESP	126	ESP (SPI=0xee294764)
22	29.271825	192.168.6.2	192.168.4.2	ESP	126	ESP (SPI=0xeea0e03f)
24	30.239608	192.168.4.2	192.168.6.2	ESP	126	ESP (SPI=0xee294764)
25	30.271690	192.168.6.2	192.168.4.2	ESP	126	ESP (SPI=0xeea0e03f)
26	31.239607	192.168.4.2	192.168.6.2	ESP	126	ESP (SPI=0xee294764)
27	31.271618	192.168.6.2	192.168.4.2	ESP	126	ESP (SPI=0xeea0e03f)
124	92.506562	192.168.4.2	192.168.6.2	ESP	126	ESP (SPI=0xee294764)
125	92.745941	192.168.6.2	192.168.4.2	ESP	110	ESP (SPI=0xeea0e03f)

**Gambar 4.14**  
**Wireshark pada VPN**

Pada jaringan dengan Virtual Private Network, wireshark hanya mendeteksi paket-paket ESP dengan alamat IP yang dimiliki oleh kedua gateway VPN saja. Hasil capture pada jaringan VPN dapat dilihat pada gambar 4.14. Berdasarkan gambar tersebut, diperoleh fakta-fakta sebagai berikut:

- Tidak ada alamat IP komputer pengirim dan komputer penerima pada wireshark. Yang terdeteksi hanya alamat IP gateway VPN.
- Tidak ada paket TCP/IP (yang digunakan oleh program) yang terdeteksi oleh wireshark. Yang terdeteksi hanya paket ESP.
- Tidak terdapat paket dengan port 8080 (yang digunakan oleh program) yang terdeteksi oleh wireshark.

Hal tersebut membuktikan bahwa setiap paket data yang keluar dari gateway VPN, akan mengalami enkapsulasi menjadi sebuah paket ESP, di mana paket tersebut dikirimkan menuju gateway VPN tujuan yang kemudian menerjemahkan kembali paket tersebut menjadi paket asal.

### 4.3. Metode Penelitian

Untuk mengambil kesimpulan dalam studi analisa ini digunakan dua buah model statistik, yaitu ANOVA (Analysis of Variance) dan Regresi Linear. Dan akan disertakan sebuah analisa biaya yang membandingkan antara biaya untuk pembangunan VPN dengan biaya untuk teknologi WAN yang lainnya.

#### 4.3.1. ANOVA (Analysis of Variance)

ANOVA merupakan sebuah metode analisis statistika yang termasuk ke dalam cabang statistika inferensi. Dalam literatur Indonesia, metode ini dikenal dengan berbagai nama, seperti analisis ragam, sidik ragam, dan analisis variansi.

ANOVA merupakan sebuah metode yang digunakan dalam pengambilan keputusan. ANOVA pertama kali diperkenalkan oleh Sir Ronald Fisher. Dalam prakteknya, ANOVA dapat berupa uji hipotesis, maupun pendugaan.

Secara umum, ANOVA menguji dua varians berdasarkan hipotesis not bahwa kedua varians itu sama. Varians pertama adalah varians antar contoh (among samples), dan varians kedua adalah varians di dalam masing-masing contoh (within samples). Dengan ide semacam ini, analisis varians dengan dua contoh akan memberikan hasil yang sama dengan uji-t untuk dua mean atau rata-rata.

Terdapat empat buah asumsi yang harus terpenuhi agar hasilnya dapat dianggap sah:

1. Data berdistribusi normal
2. Varians bersifat homogen
3. Masing-masing contoh bersifat independen
4. Komponen-komponen bersifat aditif

ANOVA relatif mudah untuk dimodifikasi dan dapat dikembangkan untuk berbagai bentuk percobaan yang rumit. Penggunaan ANOVA sangat luas di berbagai bidang, mulai dari eksperimen laboratorium, periklanan, psikologi, hingga kemasyarakatan.

Tujuan utama ANOVA adalah pembuktian terhadap sebuah hipotesis yang bersifat praduga. Hipotesis tersebut, dalam ANOVA disebut dengan  $H_0$ . Sehingga dalam kesimpulannya nanti yang akan diperoleh adalah “ $H_0$  diterima”, atau “ $H_0$  ditolak”.

Pengambilan keputusan terhadap hipotesis ANOVA, dilakukan berdasarkan perbandingan dari nilai F hitung yang diperoleh pada tabel ANOVA, dengan nilai F tabel distribusi F (Fisher), pada baris dan kolom tabel tersebut berdasarkan nilai df (degree of freedom) varian dan df error. Apabila  $F_{hitung} < F_{tabel}$ , maka  $H_0$  diterima, sedangkan  $H_0$  ditolak apabila  $F_{hitung} > F_{tabel}$ .

#### 4.3.2. Regresi Linear

Regresi linear merupakan sebuah alat statistik yang dipergunakan untuk mengetahui pengaruh antara satu atau beberapa variabel terhadap satu buah variabel. Variabel yang mempengaruhi sering disebut variabel bebas, variabel independen atau variabel penjelas. Variabel yang dipengaruhi sering disebut dengan variabel terikat atau variabel dependen. Regresi linear hanya dapat digunakan pada skala interval dan rasio.

Analisis regresi linear sederhana dipergunakan untuk mengetahui pengaruh antara satu buah variabel bebas terhadap satu buah variabel terikat. Dengan menggunakan persamaan umum:

$$Y = a + b X \quad \dots\dots\dots (4.1)$$

Di mana Y adalah variabel terikat dan X adalah variabel bebas. Koefisien a adalah konstanta (intercept) yang merupakan titik potong antara garis regresi dengan sumbu Y pada koordinat kartesius. Garis regresi adalah garis linear yang menunjukkan pola hubungan antara X dan Y, yang sebenarnya merupakan garis taksiran yang dipakai untuk mewakili pola sebaran data.

Dalam regresi terdapat dua buah ukuran atau koefisien, yaitu koefisien regresi dan koefisien korelasi. Koefisien regresi mengukur besarnya pengaruh X (variabel bebas) terhadap Y (variabel terikat). Sedangkan korelasi mengukur kuat tidaknya hubungan X dan Y.

Dengan menggunakan metode regresi linear ini, diharapkan dapat disimpulkan sebuah fungsi persamaan yang dapat menggambarkan hubungan antara jumlah router pada WAN dengan performa tunnel VPN IPsec yang terbentuk oleh masing-masing kombinasi. Di mana kecepatan PING dapat diperkirakan dengan sebuah persamaan yang diaplikasikan pada jumlah router yang digunakan.

#### **4.4. Uji Coba dan Analisa**

Dengan skenario uji coba, metode penelitian, serta tolak ukur yang telah dijelaskan sebelumnya, maka studi analisa ini dapat dimulai.

##### **4.4.1. Uji Coba**

Terdapat enam kombinasi yang digunakan, yaitu DES-SHA, DES-MD5, 3DES-SHA, 3DES-MD5, AES-SHA, dan AES-MD5. Ditambah dengan sebuah kombinasi, yang tidak menggunakan enkripsi, maupun hash. Kombinasi ini berfungsi sebagai sebuah variabel kontrol.

##### **4.4.1.1. DES-SHA**

Kombinasi ini membentuk VPN menggunakan autentikasi pre-shared key dengan key “cisco”, enkripsi DES, dan hash SHA. Dengan demikian konfigurasi yang harus dilakukan pada Router 1 dapat dilihat pada listing berikut ini.

##### **Listing 4.4 Konfigurasi Umum DES-SHA Router 1**

```

1 : R1(config)# crypto isakmp policy 10
2 : R1(config-isakmp)# authentication pre-share
3 : R1(config-isakmp)# encryption des
4 : R1(config-isakmp)# hash sha
5 : R1(config-isakmp)# group 5
6 : R1(config-isakmp)# lifetime 3600
7 : R1(config-isakmp)# exit
8 : R1(config)# crypto isakmp key cisco address 192.168.6.2
9 : R1(config)# crypto ipsec transform-set 50 esp-des esp-sha-
    hmac ah-sha-hmac
10 : R1(cfg-crypto-trans)# exit

```

Sedangkan berikut ini adalah konfigurasi umum yang harus dilakukan pada Router 2.

**Listing 4.5 Konfigurasi Umum DES-SHA Router 2**

```

1 : R2(config)# crypto isakmp policy 10
2 : R2(config-isakmp)# authentication pre-share
3 : R2(config-isakmp)# encryption des
4 : R2(config-isakmp)# hash sha
5 : R2(config-isakmp)# group 5
6 : R2(config-isakmp)# lifetime 3600
7 : R2(config-isakmp)# exit
8 : R2(config)# crypto isakmp key cisco address 192.168.4.2
9 : R2(config)# crypto ipsec transform-set 50 esp-des esp-sha-
    hmac ah-sha-hmac
10 : R2(cfg-crypto-trans)# exit

```

Setelah dilakukan konfigurasi terhadap metode enkripsi, autentikasi, hash, algoritma DH, serta pembentukan IPsec transform-set, perlu dilakukan tahap konfigurasi pasca konfigurasi umum. Pasca konfigurasi juga digunakan pada kombinasi-kombinasi yang lainnya. Berikut ini pasca konfigurasi yang harus dilakukan pada Router 1.

**Listing 4.6Pasca Konfigurasi Router 1**

```

1 : R1(config)# access-list 101 permit ip 202.154.17.0 0.0.0.255
    202.154.18.0 0.0.0.255
2 : R1(config)# crypto map STTS 10 ipsec-isakmp
3 : % NOTE: This new crypto map will remain disabled until a
    peer
        and a valid access list have been configured.
4 : R1(config-crypto-map)# match address 101
5 : R1(config-crypto-map)# set peer 192.168.6.2
6 : R1(config-crypto-map)# set pfs group5
7 : R1(config-crypto-map)# set transform-set 50
8 : R1(config-crypto-map)# set security-association lifetime
    seconds 900
9 : R1(config-crypto-map)# exit
10 : R1(config)# interface fastethernet0/0
11 : R1(config-if)# crypto map STTS
12 : *Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
13 : R1(config-if)# exit

```

Selain pasca konfigurasi pada Router 1, juga harus dilakukan pasca konfigurasi pada Router 2. berikut ini adalah pasca konfigurasi yang harus dilakukan pada Router 2.

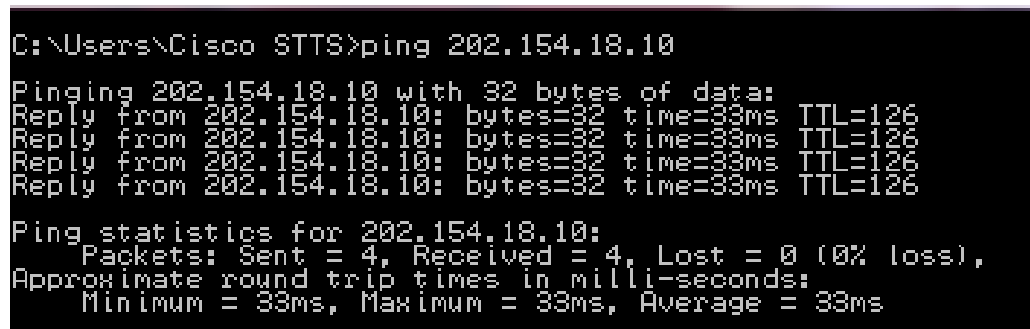
**Listing 4.7 Pasca Konfigurasi Router 2**

```

1 : R1(config)# access-list 101 permit ip 202.154.17.0 0.0.0.255
    202.154.18.0 0.0.0.255
2 : R1(config)# crypto map STTS 10 ipsec-isakmp
3 : % NOTE: This new crypto map will remain disabled until a
    peer
        and a valid access list have been configured.
4 : R1(config-crypto-map)# match address 101
5 : R1(config-crypto-map)# set peer 192.168.6.2
6 : R1(config-crypto-map)# set pfs group5
7 : R1(config-crypto-map)# set transform-set 50
8 : R1(config-crypto-map)# set security-association lifetime
    seconds 900
9 : R1(config-crypto-map)# exit
10 : R1(config)# interface fastethernet0/0
11 : R1(config-if)# crypto map STTS
12 : *Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
13 : R1(config-if)# exit

```

Dari 4 PING yang dilakukan pada kombinasi DES-SHA pada WAN 2 Router, diperoleh PING dengan kecepatan minimum 33ms, maksimum 33 ms, dan rata-rata 33ms. Adapun performa PING dari kombinasi DES-SHA dapat dilihat pada gambar berikut ini.



```

C:\Users\Cisco STTS>ping 202.154.18.10

Pinging 202.154.18.10 with 32 bytes of data:
Reply from 202.154.18.10: bytes=32 time=33ms TTL=126
Reply from 202.154.18.10: bytes=32 time=33ms TTL=126
Reply from 202.154.18.10: bytes=32 time=33ms TTL=126
Reply from 202.154.18.10: bytes=32 time=33ms TTL=126

Ping statistics for 202.154.18.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 33ms, Maximum = 33ms, Average = 33ms

```

**Gambar 4.15**  
**PING Kombinasi DES-SHA 2 Router**

Pada wireshark yang terletak pada perangkat penyadap, dengan filter berdasarkan alamat IP dan port, tidak terdeteksi adanya paket data yang melintas. Namun jika filter diubah menjadi alamat IP yang dimiliki oleh router gateway VPN, akan terdeteksi adanya paket data yang melintas. Paket tersebut tidak berprotokol TCP, namun terenkapsulasi menjadi sebuah paket ESP yang merupakan paket dengan protokol Encapsulated Security Payload.

Filter: (ip.addr==192.168.6.2) Expression... Clear Apply						
No.	Time	Source	Destination	Protocol	Length	Info
19	28.243978	192.168.4.2	192.168.6.2	ESP	126	ESP (SPI=0xee294764)
20	28.276374	192.168.6.2	192.168.4.2	ESP	126	ESP (SPI=0xeea0e03f)
21	29.239572	192.168.4.2	192.168.6.2	ESP	126	ESP (SPI=0xee294764)
22	29.271825	192.168.6.2	192.168.4.2	ESP	126	ESP (SPI=0xeea0e03f)
24	30.239608	192.168.4.2	192.168.6.2	ESP	126	ESP (SPI=0xee294764)
25	30.271690	192.168.6.2	192.168.4.2	ESP	126	ESP (SPI=0xeea0e03f)
26	31.239607	192.168.4.2	192.168.6.2	ESP	126	ESP (SPI=0xee294764)
27	31.271618	192.168.6.2	192.168.4.2	ESP	126	ESP (SPI=0xeea0e03f)
124	92.506562	192.168.4.2	192.168.6.2	ESP	126	ESP (SPI=0xee294764)
125	92.745941	192.168.6.2	192.168.4.2	ESP	110	ESP (SPI=0xeea0e03f)

**Gambar 4.16**  
**Paket ESP Pada Wireshark**

#### 4.4.1.2. DES-MD5

Kombinasi ini membentuk VPN menggunakan autentikasi pre-shared key dengan key “cisco”, enkripsi DES, dan hash MD5. Dengan demikian konfigurasi yang harus dilakukan pada kedua router dapat dilihat pada listing berikut ini.

##### Listing 4.8 Konfigurasi Umum DES-MD5 Router 1

```

1 : R1(config)# crypto isakmp policy 10
2 : R1(config-isakmp)# authentication pre-share
3 : R1(config-isakmp)# encryption des
4 : R1(config-isakmp)# hash md5
5 : R1(config-isakmp)# group 5
6 : R1(config-isakmp)# lifetime 3600
7 : R1(config-isakmp)# exit
8 : R1(config)# crypto isakmp key cisco address 192.168.6.2
9 : R1(config)# crypto ipsec transform-set 50 esp-des esp-md5-
    hmac
10 : R1(cfg-crypto-trans)# exit

```

Sedangkan berikut ini adalah konfigurasi umum yang harus dilakukan pada Router 2.

##### Listing 4.9 Konfigurasi Umum DES-MD5 Router 2

```

1 : R2(config)# crypto isakmp policy 10
2 : R2(config-isakmp)# authentication pre-share
3 : R2(config-isakmp)# encryption des
4 : R2(config-isakmp)# hash md5
5 : R2(config-isakmp)# group 5
6 : R2(config-isakmp)# lifetime 3600
7 : R2(config-isakmp)# exit
8 : R2(config)# crypto isakmp key cisco address 192.168.4.2
9 : R2(config)# crypto ipsec transform-set 50 esp-des esp-md5-
    hmac
10 : R2(cfg-crypto-trans)# exit

```

Dari 4 PING yang dilakukan pada kombinasi DES-MD5 pada WAN 2 Router, diperoleh PING dengan kecepatan minimum 33ms, maksimum 33 ms, dan rata-rata 33ms. Adapun performa PING dari kombinasi DES-SHA dapat dilihat pada gambar di bawah ini.

```
C:\Users\Cisco STTS>ping 202.154.18.10

Pinging 202.154.18.10 with 32 bytes of data:
Reply from 202.154.18.10: bytes=32 time=33ms TTL=126
Reply from 202.154.18.10: bytes=32 time=33ms TTL=126
Reply from 202.154.18.10: bytes=32 time=32ms TTL=126
Reply from 202.154.18.10: bytes=32 time=33ms TTL=126

Ping statistics for 202.154.18.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 32ms, Maximum = 33ms, Average = 32ms
```

**Gambar 4.17**  
**PING Kombinasi DES-MD5 2 Router**

#### 4.4.1.3. 3DES-SHA

Kombinasi ini membentuk VPN menggunakan autentikasi pre-shared key dengan key “cisco”, enkripsi 3DES, dan hash SHA. Dengan demikian konfigurasi yang harus dilakukan pada kedua router dapat dilihat pada listing berikut ini.

##### **Listing 4.10 Konfigurasi Umum 3DES-SHA Router 1**

```
1 : R1(config)# crypto isakmp policy 10
2 : R1(config-isakmp)# authentication pre-share
3 : R1(config-isakmp)# encryption 3des
4 : R1(config-isakmp)# hash sha
5 : R1(config-isakmp)# group 5
6 : R1(config-isakmp)# lifetime 3600
7 : R1(config-isakmp)# exit
8 : R1(config)# crypto isakmp key cisco address 192.168.6.2
9 : R1(config)# crypto ipsec transform-set 50 esp-3des esp-sha-
    hmac
10 : R1(cfg-crypto-trans)# exit
```

Sedangkan berikut ini adalah konfigurasi umum yang harus dilakukan pada Router 2.

##### **Listing 4.11 Konfigurasi Umum 3DES-SHA Router 2**

```
1 : R2(config)# crypto isakmp policy 10
2 : R2(config-isakmp)# authentication pre-share
3 : R2(config-isakmp)# encryption 3des
4 : R2(config-isakmp)# hash sha
```



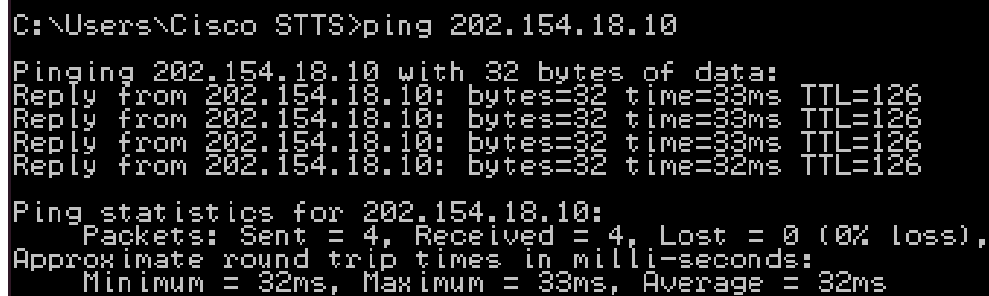
**Listing 4.11 Konfigurasi Umum 3DES-SHA Router 2 (lanjutan)**

```

5 : R2(config-isakmp)# group 5
6 : R2(config-isakmp)# lifetime 3600
7 : R2(config-isakmp)# exit
8 : R2(config)# crypto isakmp key cisco address 192.168.4.2
9 : R2(config)# crypto ipsec transform-set 50 esp-3des esp-sha-
    hmac
10 : R2(cfg-crypto-trans)# exit

```

Dari 4 PING yang dilakukan pada kombinasi 3DES-SHA pada WAN 2 Router, diperoleh PING dengan kecepatan minimum 33ms, maksimum 33 ms, dan rata-rata 33ms. Adapun performa PING dari kombinasi DES-SHA dapat dilihat pada gambar di bawah ini.



```

C:\Users\Cisco STTS>ping 202.154.18.10

Pinging 202.154.18.10 with 32 bytes of data:
Reply from 202.154.18.10: bytes=32 time=33ms TTL=126
Reply from 202.154.18.10: bytes=32 time=33ms TTL=126
Reply from 202.154.18.10: bytes=32 time=33ms TTL=126
Reply from 202.154.18.10: bytes=32 time=32ms TTL=126

Ping statistics for 202.154.18.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 32ms, Maximum = 33ms, Average = 32ms

```

**Gambar 4.18**  
**PING Kombinasi 3DES-SHA 2 Router**

**4.4.1.4. 3DES-MD5**

Kombinasi ini membentuk VPN menggunakan autentikasi pre-shared key dengan key “cisco”, enkripsi 3DES, dan hash MD5. Dengan demikian konfigurasi yang harus dilakukan pada kedua router dapat dilihat pada listing berikut ini.

**Listing 4.12 Konfigurasi Umum 3DES-MD5 Router 1**

```

1 : R1(config)# crypto isakmp policy 10
2 : R1(config-isakmp)# authentication pre-share
3 : R1(config-isakmp)# encryption 3des
4 : R1(config-isakmp)# hash md5
5 : R1(config-isakmp)# group 5
6 : R1(config-isakmp)# lifetime 3600
7 : R1(config-isakmp)# exit
8 : R1(config)# crypto isakmp key cisco address 192.168.6.2
9 : R1(config)# crypto ipsec transform-set 50 esp-des esp-md5-
    hmac
10 : R1(cfg-crypto-trans)# exit

```

Sedangkan berikut ini adalah konfigurasi umum yang harus dilakukan pada Router 2.

**Listing 4.13 Konfigurasi Umum 3DES-MD5 Router 2**

```

1 : R2(config)# crypto isakmp policy 10
2 : R2(config-isakmp)# authentication pre-share
3 : R2(config-isakmp)# encryption 3des
4 : R2(config-isakmp)# hash md5
5 : R2(config-isakmp)# group 5
6 : R2(config-isakmp)# lifetime 3600
7 : R2(config-isakmp)# exit
8 : R2(config)# crypto isakmp key cisco address 192.168.4.2
9 : R2(config)# crypto ipsec transform-set 50 esp-des esp-md5-
    hmac
10 : R2(cfg-crypto-trans)# exit

```

Dari 4 PING yang dilakukan pada kombinasi 3DES-MD5 pada WAN 2 Router, diperoleh PING dengan kecepatan minimum 33ms, maksimum 33 ms, dan rata-rata 33ms. Adapun performa PING dari kombinasi DES-SHA dapat dilihat pada gambar di bawah ini.



```

C:\Users\Cisco STTS>ping 202.154.18.10

Pinging 202.154.18.10 with 32 bytes of data:
Reply from 202.154.18.10: bytes=32 time=33ms TTL=126
Reply from 202.154.18.10: bytes=32 time=32ms TTL=126
Reply from 202.154.18.10: bytes=32 time=33ms TTL=126
Reply from 202.154.18.10: bytes=32 time=33ms TTL=126

Ping statistics for 202.154.18.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 32ms, Maximum = 33ms, Average = 32ms

```

**Gambar 4.19**  
**PING Kombinasi 3DES-MD5 2 Router**

#### 4.4.1.5. AES-SHA

Kombinasi ini membentuk VPN menggunakan autentikasi pre-shared key dengan key “cisco”, enkripsi AES, dan hash SHA. Dengan demikian konfigurasi yang harus dilakukan pada kedua router dapat dilihat pada listing berikut ini.

**Listing 4.14 Konfigurasi Umum AES-SHA Router 1**

```

1 : R1(config)# crypto isakmp policy 10
2 : R1(config-isakmp)# authentication pre-share
3 : R1(config-isakmp)# encryption aes 256

```

**Listing 4.14 Konfigurasi Umum AES-SHA Router 1 (lanjutan)**

```

4 : R1(config-isakmp)# hash sha
5 : R1(config-isakmp)# group 5
6 : R1(config-isakmp)# lifetime 3600
7 : R1(config-isakmp)# exit
8 : R1(config)# crypto isakmp key cisco address 192.168.6.2
9 : R1(config)# crypto ipsec transform-set 50 esp-aes 256 esp-
    sha-hmac ah-sha-hmac
10 : R1(cfg-crypto-trans)# exit

```

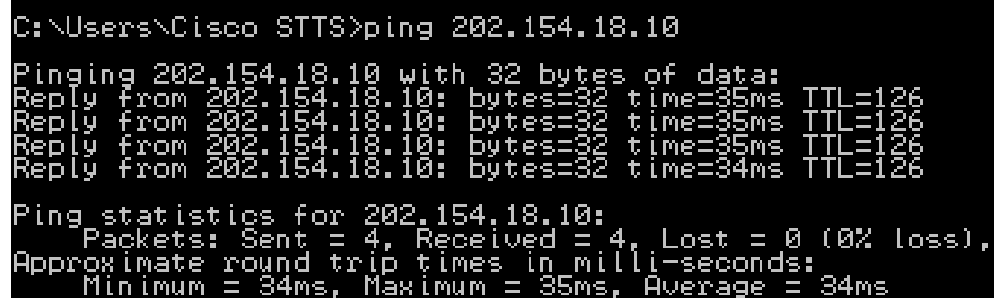
Sedangkan berikut ini adalah konfigurasi umum yang harus dilakukan pada Router 2.

**Listing 4.15 Konfigurasi Umum AES-SHA Router 2**

```

1 : R2(config)# crypto isakmp policy 10
2 : R2(config-isakmp)# authentication pre-share
3 : R2(config-isakmp)# encryption aes 256
4 : R2(config-isakmp)# hash sha
5 : R2(config-isakmp)# group 5
6 : R2(config-isakmp)# lifetime 3600
7 : R2(config-isakmp)# exit
8 : R2(config)# crypto isakmp key cisco address 192.168.4.2
9 : R2(config)# crypto ipsec transform-set 50 esp-aes 256 esp-
    sha-hmac ah-sha-hmac
10 : R2(cfg-crypto-trans)# exit

```



```

C:\Users\Cisco STTS>ping 202.154.18.10

Pinging 202.154.18.10 with 32 bytes of data:
Reply from 202.154.18.10: bytes=32 time=35ms TTL=126
Reply from 202.154.18.10: bytes=32 time=35ms TTL=126
Reply from 202.154.18.10: bytes=32 time=35ms TTL=126
Reply from 202.154.18.10: bytes=32 time=34ms TTL=126

Ping statistics for 202.154.18.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 34ms, Maximum = 35ms, Average = 34ms

```

**Gambar 4.20**  
**PING Kombinasi AES-SHA 2 Router**

Dari 4 PING yang dilakukan pada kombinasi AES-SHA pada WAN 2 Router, diperoleh PING dengan kecepatan minimum 33ms, maksimum 33 ms, dan rata-rata 33ms. Adapun performa PING dari kombinasi DES-SHA dapat dilihat pada gambar 4.18.

#### 4.4.1.6. AES-MD5

Kombinasi ini membentuk VPN menggunakan autentikasi pre-shared key dengan key “cisco”, enkripsi AES, dan hash MD5. Dengan demikian konfigurasi yang harus dilakukan pada kedua router dapat dilihat pada listing berikut ini.

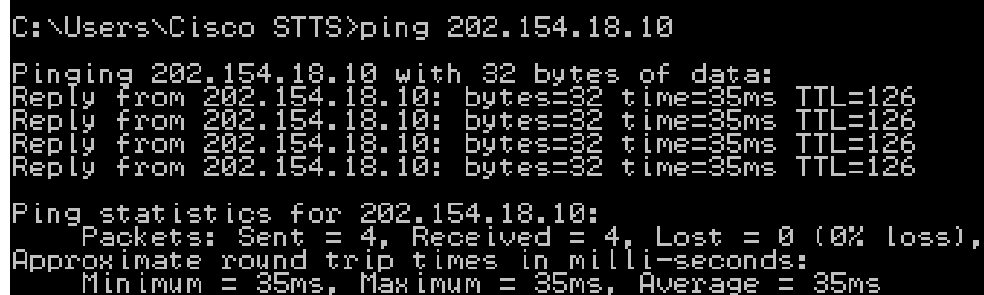
##### Listing 4.16 Konfigurasi Umum AES-MD5 Router 1

```
1 : R1(config)# crypto isakmp policy 10
2 : R1(config-isakmp)# authentication pre-share
3 : R1(config-isakmp)# encryption aes 256
4 : R1(config-isakmp)# hash md5
5 : R1(config-isakmp)# group 5
6 : R1(config-isakmp)# lifetime 3600
7 : R1(config-isakmp)# exit
8 : R1(config)# crypto isakmp key cisco address 192.168.6.2
9 : R1(config)# crypto ipsec transform-set 50 esp-aes 256 esp-
    md5-hmac ah-md5-hmac
10 : R1(cfg-crypto-trans)# exit
```

Sedangkan berikut ini adalah konfigurasi umum yang harus dilakukan pada Router 2.

##### Listing 4.17 Konfigurasi Umum AES-MD5 Router 2

```
1 : R2(config)# crypto isakmp policy 10
2 : R2(config-isakmp)# authentication pre-share
3 : R2(config-isakmp)# encryption aes 256
4 : R2(config-isakmp)# hash md5
5 : R2(config-isakmp)# group 5
6 : R2(config-isakmp)# lifetime 3600
7 : R2(config-isakmp)# exit
8 : R2(config)# crypto isakmp key cisco address 192.168.4.2
9 : R2(config)# crypto ipsec transform-set 50 esp-aes 256 esp-
    md5-hmac ah-md5-hmac
10 : R2(cfg-crypto-trans)# exit
```



```
C:\Users\Cisco STTS>ping 202.154.18.10

Pinging 202.154.18.10 with 32 bytes of data:
Reply from 202.154.18.10: bytes=32 time=35ms TTL=126
Reply from 202.154.18.10: bytes=32 time=35ms TTL=126
Reply from 202.154.18.10: bytes=32 time=35ms TTL=126
Reply from 202.154.18.10: bytes=32 time=35ms TTL=126

Ping statistics for 202.154.18.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 35ms, Maximum = 35ms, Average = 35ms
```

**Gambar 4.21**  
**PING Kombinasi AES-MD5 2 Router**

Dari 4 PING yang dilakukan pada kombinasi AES-MD5 pada WAN 2 Router, diperoleh PING dengan kecepatan minimum 33ms, maksimum 33 ms, dan rata-rata 33ms. Adapun performa PING dari kombinasi DES-SHA dapat dilihat pada gambar berikut ini.

#### 4.4.2. Analisa

Berdasarkan percobaan yang telah dilakukan pada sub-bab sebelumnya, maka diperoleh hasil dari kombinasi-kombinasi tersebut. Berikut ini tabel yang dihasilkan melalui beberapa percobaan yang sudah dilakukan sebelumnya.

**Tabel 4.3**  
**Tabel Hasil Uji Coba**

No	Encr	Hash	0 Router Pass	2 Router Pass	6 Router Pass
0	No VPN		1ms	18ms	87ms
			1ms	18ms	87ms
			1ms	18ms	87ms
1	DES	SHA	2ms	33ms	156ms
			2ms	24ms	169ms
			2ms	33ms	164ms
2	DES	MD5	2ms	33ms	155ms
			1ms	35ms	158ms
			2ms	33ms	158ms
3	3DES	SHA	2ms	33ms	155ms
			2ms	33ms	155ms
			2ms	33ms	155ms
4	3DES	MD5	2ms	32ms	156ms
			2ms	33ms	159ms
			2ms	33ms	155ms
5	AES	SHA	2ms	35ms	166ms
			1ms	36ms	167ms
			2ms	35ms	166ms
6	AES	MD5	2ms	35ms	166ms
			2ms	35ms	166ms
			1ms	35ms	166ms

Dari tabel tersebut, terdapat data dari kombinasi-kombinasi IPsec. Dari data tersebut terdapat 1 sampel tanpa VPN, dan 6 sampel kombinasi VPN IPsec.

Sehingga jika dibedakan menjadi dua, antara data tanpa VPN dan data VPN IPsec. Dengan menghitung rata-rata dari ketiga sampel dari masing-masing kombinasi untuk percobaan tanpa VPN. Dan menghitung rata-rata dari sampel VPN pada masing-masing jumlah router yang dilewati, 0 router, 2 router, dan 6 router. Sehingga tabel 4.3 tersebut dapat disederhanakan menjadi tabel 4.4 berikut ini.

**Tabel 4.4**  
**Tabel Perbandingan VPN dan Tanpa VPN**

No	Methods	0 Router Pass	2 Router Pass	6 Router Pass
1	No VPN	1	18	87
2	VPN IPsec	1.833333333	33.27777778	160.6666667
	Ratio	1.833333333	1.848765432	1.846743295

Berdasarkan tabel tersebut, dapat dilihat peningkatan waktu dari performa PING VPN IPsec dengan rasio penurunan rata-rata 1.8 kali lebih lama, atau menurun sekitar 44,44% dari jaringan normal tanpa VPN.

#### 4.4.2.1. ANOVA

Dari hasil percobaan yang telah diperoleh, dilakukan proses input ke dalam tabel ANOVA. Variabel yang diinputkan ke dalam tabel ANOVA hanya sebatas kecepatan PING saja, karena hasil keamanan paket relatif sama.

Pada studi analisa ini, diambil 7 buah hipotesis ( $H_0$ ), yaitu:

- $H_{0(1)}$  = Jumlah router pada WAN tidak berpengaruh pada performa VPN  
 $H_{1(1)}$  = Jumlah router pada WAN berpengaruh pada performa VPN
- $H_{0(2)}$  = Metode hash tidak berpengaruh pada performa VPN  
 $H_{1(2)}$  = Metode hash berpengaruh pada performa VPN
- $H_{0(3)}$  = Metode enkripsi tidak berpengaruh pada performa VPN  
 $H_{1(3)}$  = Metode enkripsi berpengaruh pada performa VPN
- $H_{0(4)}$  = Interaksi antara metode hash dengan jumlah router pada WAN tidak berpengaruh pada performa VPN  
 $H_{1(4)}$  = Interaksi antara metode hash dengan jumlah router pada WAN berpengaruh pada performa VPN

- $H_{0(5)}$  = Interaksi antara metode enkripsi dengan jumlah router pada WAN berpengaruh pada performa VPN  
 $H_{1(5)}$  = Interaksi antara metode enkripsi dengan jumlah router pada WAN berpengaruh pada performa VPN
- $H_{0(6)}$  = Interaksi antara metode hash dengan metode enkripsi tidak berpengaruh pada performa VPN  
 $H_{1(6)}$  = Interaksi antara metode hash dengan metode enkripsi berpengaruh pada performa VPN
- $H_{0(7)}$  = Interaksi antara metode hash, metode enkripsi, dan jumlah router pada WAN tidak berpengaruh pada performa VPN  
 $H_{1(7)}$  = Interaksi antara metode hash, metode enkripsi, dan jumlah router pada WAN berpengaruh pada performa VPN

Berdasarkan tabel hasil percobaan yang telah diperoleh, dilakukan perhitungan ANOVA dengan menggunakan bantuan perangkat lunak SPSS Statistics 17.0. Adapun tiga faktor utama yang digunakan sebagai acuan, yaitu Enkripsi, Hash, dan jumlah router pada WAN. Berikut ini hasil dari perhitungan ANOVA tersebut.

**Tabel 4.5**  
**Tabel ANOVA – Faktor Antar Subyek**

		Value Label	N
Router	.00	WAN 0 Router	18sampel
	2.00	WAN 2 Router	18sampel
	6.00	WAN 6 Router	18sampel
Hash	1.00	SHA1	27sampel
	2.00	MD5	27sampel
Enkripsi	1.00	DES	18sampel
	2.00	3DES	18sampel
	3.00	AES	18sampel

Tabel 4.5 tersebut merupakan perhitungan awal terhadap sampel data yang telah diinputkan ke dalam tabel. Dapat dilihat bahwa sampel dengan subyek WAN

0 Router terdapat 18 buah sampel, begitu pula dengan WAN 2 Router serta WAN 6 Router, masing-masing 18 buah sampel. Sedangkan sampel dengan Hash SHA serta MD5, masing-masing memiliki 27 sampel percobaan. Dan subyek enkripsi, masing-masing memiliki 18 buah sampel. Data jumlah sampel tersebut kemudian digunakan untuk melakukan perhitungan berikutnya.

**Tabel 4.6**  
**Tabel ANOVA – Test Efek Antar Subyek**

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Router	253145.148	2	126572.574	37349.284	.000
Hash	.907	1	.907	.268	.608
Enkripsi	165.148	2	82.574	24.366	.000
Router * Hash	4.704	2	2.352	.694	.506
Router * Enkripsi	164.852	4	41.213	12.161	.000
Hash * Enkripsi	10.037	2	5.019	1.481	.241
Router * Hash * Enkripsi	33.519	4	8.380	2.473	.062
Error	122.000	36	3.389		
Total	484273.000	54			

Dependent Variable:PING

a. R Squared = 1.000 (Adjusted R Squared = .999)

Pada tabel tersebut komponen-komponen penyusunnya dapat dijelaskan sebagai berikut:

- Type III Sum of Squares, jumlah kuadrat marginal yang diperoleh dari jumlah faktor pada tabel hasil analisa
- df (degree of freedom), derajat kebebasan
- Mean Square, rata-rata kuadrat yang diperoleh dari Type III Sum of Squares dibagi dengan degree of freedom.
- F hitung (F), diperoleh dari Mean Square faktor dibagi dengan Mean Square Error
- Significat Factor (Sig.), Faktor yang menentukan keakuaratan perhitungan.



- Error df, merupakan selisih nilai antara jumlah degree of freedom dari faktor, dengan total jumlah sampel.
- Total, total dari masing-masing kolom.

Dengan mendapatkan nilai F hitung pada tabel di atas, maka uji hipotesis dapat dilakukan dengan mengacu pada tabel distribusi F dengan probabilitas 0.05 yang terlampir pada Lampiran X.

- $H_{0(1)}$  = Jumlah router pada WAN tidak berpengaruh pada performa VPN  
 $H_{1(1)}$  = Jumlah router pada WAN berpengaruh pada performa VPN

- Jika F hitung < F tabel,  $H_{0(1)}$  diterima
- Jika F hitung > F tabel,  $H_{0(1)}$  ditolak

df Router = 2

df error = 36

F hitung = 37349.284

F tabel(2,36) = 3.26

Significant Factor = 0.000

Keputusan:

Terlihat bahwa F hitung = 37349.284 dan F tabel = 3.26. Oleh karena F hitung > F tabel, maka  $H_{0(1)}$  ditolak atau jumlah router pada WAN berpengaruh pada performa VPN.

- $H_{0(2)}$  = Metode hash tidak berpengaruh pada performa VPN  
 $H_{1(2)}$  = Metode hash berpengaruh pada performa VPN

- Jika F hitung < F tabel,  $H_{0(2)}$  diterima
- Jika F hitung > F tabel,  $H_{0(2)}$  ditolak

df Hash = 1

df error = 36

F hitung = 0.268

F tabel(1,36) = 4.11

Significant Factor = 0.608

Keputusan:

Terlihat bahwa  $F_{hitung} = 0.268$  dan  $F_{tabel} = 4.11$ . Oleh karena  $F_{hitung} < F_{tabel}$ , maka  $H_{0(2)}$  diterima atau metode hash tidak berpengaruh pada performa VPN.

- $H_{0(3)}$  = Metode enkripsi tidak berpengaruh pada performa VPN

$H_{1(3)}$  = Metode enkripsi berpengaruh pada performa VPN

- Jika  $F_{hitung} < F_{tabel}$ ,  $H_{0(3)}$  diterima
- Jika  $F_{hitung} > F_{tabel}$ ,  $H_{0(3)}$  ditolak

df Enkripsi = 2

df error = 36

$F_{hitung} = 24.366$

$F_{tabel(2,36)} = 3.26$

Significant Factor = 0.000

Keputusan:

Terlihat bahwa  $F_{hitung} = 24.366$  dan  $F_{tabel} = 3.26$ . Oleh karena  $F_{hitung} > F_{tabel}$ , maka  $H_{0(3)}$  ditolak atau metode enkripsi berpengaruh pada performa VPN.

- $H_{0(4)}$  = Interaksi antara metode hash dengan jumlah router pada WAN tidak berpengaruh pada performa VPN

$H_{1(4)}$  = Interaksi antara metode hash dengan jumlah router pada WAN berpengaruh pada performa VPN

- Jika  $F_{hitung} < F_{tabel}$ ,  $H_{0(4)}$  diterima
- Jika  $F_{hitung} > F_{tabel}$ ,  $H_{0(4)}$  ditolak

df Router \* Hash = 2

df error = 36

$F_{hitung} = 0.694$

$F_{tabel(2,36)} = 3.26$

Significant Factor = 0.506

Keputusan:

Terlihat bahwa  $F_{hitung} = 0.694$  dan  $F_{tabel} = 3.26$ . Oleh karena  $F_{hitung} < F_{tabel}$ , maka  $H_{0(4)}$  diterima atau interaksi antara metode hash dengan jumlah router pada WAN tidak berpengaruh pada performa VPN.

- $H_{0(5)}$  = Interaksi antara metode enkripsi dengan jumlah router pada WAN berpengaruh pada performa VPN

$H_{1(5)}$  = Interaksi antara metode enkripsi dengan jumlah router pada WAN berpengaruh pada performa VPN

- Jika  $F_{hitung} < F_{tabel}$ ,  $H_{0(5)}$  diterima
- Jika  $F_{hitung} > F_{tabel}$ ,  $H_{0(5)}$  ditolak

df Router \* Enkripsi = 4

df error = 36

$F_{hitung} = 12.161$

$F_{tabel(4,36)} = 2.63$

Significant Factor = 0.000

Keputusan:

Terlihat bahwa  $F_{hitung} = 12.161$  dan  $F_{tabel} = 2.63$ . Oleh karena  $F_{hitung} > F_{tabel}$ , maka  $H_{0(5)}$  ditolak atau interaksi antara metode enkripsi dengan jumlah router pada WAN berpengaruh pada performa VPN.

- $H_{0(6)}$  = Interaksi antara metode hash dengan metode enkripsi tidak berpengaruh pada performa VPN

$H_{1(6)}$  = Interaksi antara metode hash dengan metode enkripsi berpengaruh pada performa VPN

- Jika  $F_{hitung} < F_{tabel}$ ,  $H_{0(6)}$  diterima
- Jika  $F_{hitung} > F_{tabel}$ ,  $H_{0(6)}$  ditolak

df Hash \* Enkripsi = 2

df error = 36

$F_{hitung} = 1.481$

$F_{tabel(2,36)} = 3.26$

Significant Factor = 0.241

Keputusan:

Terlihat bahwa  $F_{hitung} = 1.481$  dan  $F_{tabel} = 3.26$ . Oleh karena  $F_{hitung} < F_{tabel}$ , maka  $H_{0(6)}$  diterima atau interaksi antara metode hash dengan metode enkripsi tidak berpengaruh pada performa VPN.

- $H_{0(7)}$  = Interaksi antara metode hash, metode enkripsi, dan jumlah router pada WAN tidak berpengaruh pada performa VPN

$H_{1(7)}$  = Interaksi antara metode hash, metode enkripsi, dan jumlah router pada WAN berpengaruh pada performa VPN

- Jika  $F_{hitung} < F_{tabel}$ ,  $H_{0(7)}$  diterima
- Jika  $F_{hitung} > F_{tabel}$ ,  $H_{0(7)}$  ditolak

df Router \* Hash \* Enkripsi = 4

df error = 36

$F_{hitung} = 2.473$

$F_{tabel}(4,36) = 2.63$

Significant Factor = 0.062

Keputusan:

Terlihat bahwa  $F_{hitung} = 2.473$  dan  $F_{tabel} = 2.63$ . Oleh karena  $F_{hitung} < F_{tabel}$ , maka  $H_{0(7)}$  diterima atau interaksi antarmetode hash, metode enkripsi, dan jumlah router pada WAN tidak berpengaruh pada performa VPN.

#### 4.4.2.2. Regresi Linear

Dari tabel hasil percobaan yang sudah dilakukan, terdapat perbedaan yang cukup signifikan pada kecepatan PING antara koneksi non VPN dengan koneksi VPN. Dari hasil tersebut pula, dapat dilihat juga bahwa faktor yang mempengaruhi kecepatan PING terletak pada faktor jumlah router yang terdapat pada WAN. Sedangkan kombinasi metode-metode IPSec, tidak banyak berpengaruh bagi performa tunnel VPN karena hasilnya relatif sama.

Dengan demikian terbentuklah sebuah tabel yang berisi hasil uji coba VPN dengan kombinasi-kombinasi yang telah dilakukan, dengan rata-rata PING dari masing-masing kombinasi.

**Tabel 4.7**  
**Tabel Rata-Rata Waktu Hasil Uji Coba**

No	Kombinasi	0 Router	2 Router	6 Router
1	DES-SHA	2	30	163
2	DES-MD5	1.666667	33.66667	157
3	3DES-SHA	2	33	155
4	3DES-MD5	2	32.66667	156.6667
5	AES-SHA	1.666667	35.33333	166.3333
6	AES-MD5	1.666667	35	166

<b>Rata-rata (ms)</b>	1.833333	33.27778	160.6667
-----------------------	----------	----------	----------

Dengan diperolehnya nilai rata-rata pada tabel 4.7 tersebut, maka fungsi regresi linear sederhana dapat dilakukan. Dengan memasukkan data rata-rata waktu tersebut pada perhitungan regresi, maka grafik regresi linear akan berbentuk seperti gambar di bawah ini:

### Pengaruh Jumlah Router Pada Performa VPN IPSec

Forecasting

Regression/Trend analysis

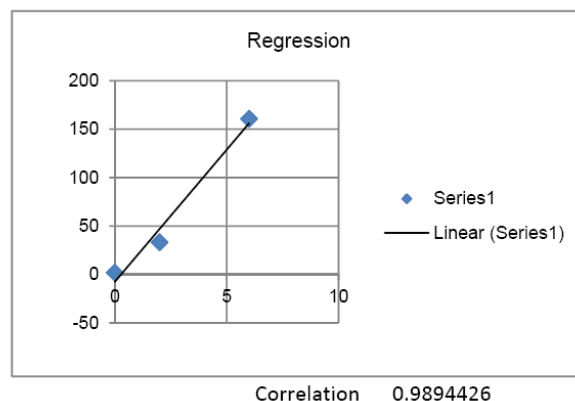
Data

Period	Demand (y)	Period(x)
Period 1	1.833333333	0
Period 2	33.27777778	2
Period 3	160.6666667	6

Intercept -7.38095238

Slope 27.24007937

Next period 101.5793651 4



**Gambar 4.22**  
**Regresi Linear**

Pada tabel tersebut, nilai waktu dimasukkan ke dalam kolom demand (y), sedangkan jumlah router dimasukkan ke dalam kolom period (x). Dari hasil operasi regresi linear tersebut, diperoleh nilai Intercept dan Slope. Intercept merupakan nilai y pada titik  $x=0$ . Slope merupakan nilai tangen dari sudut yang dibentuk oleh garis hasil regresi dengan sumbu x. Sedangkan correlation atau

korelasi merupakan sebuah ukuran kekuatan hubungan linear antara dua variabel acak, dalam hal ini x dan y. Jika nilai korelasi semakin mendekati 1, maka semakin erat hubungan asosiasi antara variabel x dan y.

Dalam persamaan umum regresi linear, Intercept disimbolkan dengan A, dan Slope disimbolkan dengan B. Sehingga jika dimasukkan ke dalam persamaan umum, maka akan diperoleh persamaan:

$$Y = -7.38 + 27.24(X) \dots\dots\dots (4.2)$$

Sehingga jika terdapat sebuah kasus VPN dengan WAN 8 Router, dapat diperkirakan kecepatan PING yang dicapai, yaitu:

$$Y = -7.38 + 27.24(8)$$

$$Y = -7.38 + 217.92 \dots\dots\dots (4.3)$$

$$Y = 210.54 = 211$$

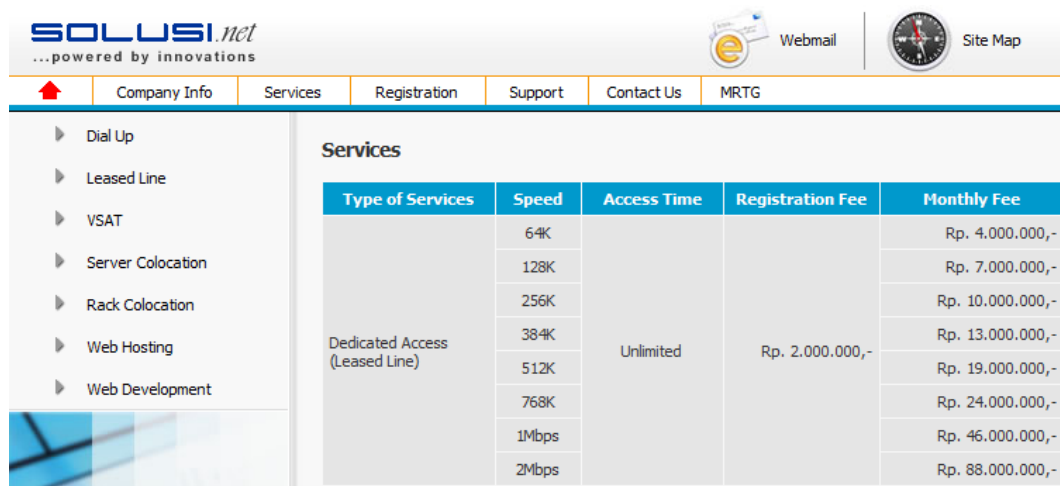
Dengan nilai korelasi 0.989, maka dapat diambil kesimpulan bahwa kedua variabel tersebut memiliki asosiasi. Sehingga jumlah router yang dilalui pada WAN mempengaruhi performa dan kinerja VPN.

#### **4.4.2.3. Analisa Biaya**

Biaya untuk membentuk sebuah VPN relatif lebih terjangkau dibandingkan menggunakan teknologi WAN yang lainnya untuk membentuk jalur komunikasi yang aman. Dalam analisa biaya ini, digunakan teknologi leased line sebagai pembanding.

Secara umum, sebuah koneksi leased line dapat digambarkan dengan memasang sebuah jalur langsung antara dua buah titik. Apabila jarak dua buah titik tersebut berdekatan, maka tidak dibutuhkan biaya yang cukup besar dalam membentuk jalur leased line tersebut. Namun apabila kedua titik tersebut berjauhan mencapai satu kilometer, maka biaya yang dibutuhkan juga tidak cukup kecil, mengingat keamanan dan performa yang dibutuhkan juga harus dapat menunjang komunikasi di antara kedua titik tersebut. Media juga menjadi masalah apabila dikaitkan dengan jarak, karena adanya line attenuation.

Gambar berikut ini, merupakan daftar biaya yang dibutuhkan untuk membentuk sebuah jaringan leased line melalui penyedia layanan Wyenet “<http://www.wyenet.net/business/leased.html>”.



Type of Services	Speed	Access Time	Registration Fee	Monthly Fee
Dedicated Access (Leased Line)	64K	Unlimited	Rp. 2.000.000,-	Rp. 4.000.000,-
	128K			Rp. 7.000.000,-
	256K			Rp. 10.000.000,-
	384K			Rp. 13.000.000,-
	512K			Rp. 19.000.000,-
	768K			Rp. 24.000.000,-
	1Mbps			Rp. 46.000.000,-
	2Mbps			Rp. 88.000.000,-

**Gambar 4.23**  
**Tarif Leased Line Solusi.Net**

Pada gambar tersebut, dapat dilihat bahwa biaya registrasi awal pembentukan jaringan leased line sebesar Rp2.000.000 untuk semua bandwidth. Sedangkan biaya bulanan bervariasi, berbanding lurus dengan bandwidth yang disediakan. Dalam kasus ini, digunakan bandwidth 2Mbps dengan biaya per bulan Rp88.000.000.

Untuk membentuk jaringan VPN melalui ADSL, diperlukan layanan ADSL sebagai penghubung menuju jaringan WAN. Gambar berikut ini merupakan daftar tarif untuk layanan ADSL Telkom Speedy dari website “<http://telkomspeedy.com/paket-harga>”.

1. Paket Speedy MultiSpeed

No.	Paket	Biaya Registrasi	Biaya Bulanan	Kuota Bulanan
1	Speedy 384 Kbps	Rp75.000	Rp195.000	Unlimited, dengan fair usage 3GB
2	Speedy 512 Kbps	Rp75.000	Rp295.000	Unlimited, dengan fair usage 3GB
3	Speedy 1 Mbps	Rp75.000	Rp645.000	Unlimited
4	Speedy 2 Mbps	Rp75.000	Rp995.000	Unlimited
5	Speedy 3 Mbps	Rp75.000	Rp1.695.000	Unlimited

**Gambar 4.24**  
**Tarif Layanan ADSL Telkom Speedy**

Dari gambar tersebut, biaya registrasi awal sebesar Rp75.000 untuk semua paket. Sedangkan biaya bulanan bervariasi, berbanding lurus dengan paket bandwidth yang disediakan. Dalam kasus ini, digunakan bandwidth 2Mbps dengan biaya per bulan Rp995.000. daftar tarif tersebut berlaku untuk satu lokasi saja.

Selain layanan ADSL, diperlukan juga router sebagai gateway VPN. Dalam analisa ini digunakan Router Cisco 1841 sebagai gateway VPN. Berikut ini harga dari Router Cisco 1841 dari “<http://www.router-switch.com>”.



**CISCO1841**  
Item #: CISCO1841 Cisco 1841 Router

★★★★★ ( 11 customer reviews )

100% SECURE 1 Year BEST PRICE 100% money back GUARANTEE PayPal WORLD WELDER

Product detail: Cisco 1800 Series Router: Cisco 1841 Modular Router w/2xFE, 2 WAN slots, 64 FL/256 DR

Conditions: New Sealed

List Price: US\$1,395.00

Unit Price: **US\$ 558.00** [Change Currency](#) ▼

Total Cost [?]: **US\$558.00** (60% off list price)

Quantity:  [Stock Available](#)

[See More 2 Images >>](#)

Shipping cost:

**Gambar 4.25**  
**Harga Router Cisco 1841**

Pada gambar di atas, harga sebuah Router Cisco 1841 baru, tanpa diskon berkisar US\$1.395. Dalam kurs dolar Amerika Rp9.500/dolar, maka harga router tersebut berkisar Rp13.252.500.

**Tabel 4.8**  
**Tabel Perbandingan Leased Line dan VPN**

Cost	Leased Line		VPN	
One Time Cost	Registratior Fee	Rp2,000,000	Registratior Fee	Rp150,000
			Cisco 1841 Router	Rp26,505,000
Periodic Cost (Mothly)				
	Mothly Fee	Rp88,000,000	Mothly Fee	Rp1,990,000
1st year	Rp1,058,000,000		Rp50,535,000	
2nd year	Rp1,056,000,000		Rp23,880,000	



Pada tabel tersebut, dapat dilihat biaya yang dibutuhkan untuk membentuk sebuah jalur komunikasi yang aman untuk bandwidth 2MB melalui provider Solusi.Net. Dengan biaya registrasi awal sebesar Rp2.000.000 dan sewa per bulan mencapai Rp88.000.000, maka pengeluaran pada tahun pertama berkisar Rp1.506.000.000.

Dengan demikian, secara kasat mata dapat diketahui bahwa VPN lebih terjangkau daripada leased line. Adapun penghematan yang dihasilkan sebesar:

$$E = \frac{100 - \left( \frac{50.535.000}{1.058.000.000} \times 100 \right)}{100}$$

$$E = \frac{100 - (0,0477 \times 100)}{100} \dots\dots\dots (4.4)$$

$$E = \frac{100 - 4,77}{100}$$

$$E = 95,22\%$$

Dengan demikian, pada kasus ini dapat diambil kesimpulan bahwa VPN mampu mengurangi biaya yang dibutuhkan untuk membentuk jaringan yang aman dengan efisiensi mencapai 95,22% dibandingkan leased line.

Meskipun VPN terhitung lebih murah dibandingkan dengan leased line, perusahaan skala besar lebih condong ke arah leased line. VPN lebih banyak diaplikasikan pada perusahaan kecil menengah.

#### 4.4.3. Hasil Analisa

Berdasarkan analisa yang telah dilakukan pada bab ini, dapat diambil kesimpulan:

- VPN IPsec menurunkan kinerja suatu jaringan 180%.
- Jumlah router pada WAN berpengaruh pada performa VPN.
- Metode hash tidak berpengaruh pada performa VPN.
- Metode enkripsi berpengaruh pada performa VPN.
- Interaksi antara metode hash dengan jumlah router pada WAN tidak berpengaruh pada performa VPN.

- Interaksi antara metode enkripsi dengan jumlah router pada WAN berpengaruh pada performa VPN.
- Interaksi antara metode hash dengan metode enkripsi tidak berpengaruh pada performa VPN.
- Interaksi antarmetode hash, metode enkripsi, dan jumlah router pada WAN tidak berpengaruh pada performa VPN.
- Jumlah router yang dilalui pada WAN mempengaruhi performa dan kinerja VPN IPsec, dengan asosiasi  $Y = -7.38 + 27.24(X)$ .
- VPN tergolong lebih murah dibandingkan dengan Leased Line, sehingga lebih cocok untuk diaplikasikan pada perusahaan kecil menengah.

#### **4.5. Cisco Configuration Professional**

Command Line Interface (CLI) merupakan sebuah model interface yang kurang ramah bagi pengguna, terlebih untuk menghafal perintah-perintah dari command line tersebut. Oleh karena itu, Cisco meluncurkan sebuah perangkat lunak guna mempermudah konfigurasi perangkat Cisco tersebut, dengan nama Cisco Configuration Professional. Cisco Configuration Professional (CCP) merupakan sebuah pengembangan dari Cisco Security Device Manager (Cisco SDM) yang merupakan pionir dari CCP. Pada beberapa komponen Cisco SDM, terdapat beberapa kelemahan yang akhirnya diperbaiki sehingga terbentuklah CCP. Namun pada dasarnya, prasyarat yang dibutuhkan oleh keduanya untuk dapat dijalankan pada komputer, adalah sama.

##### **4.5.1. Pengenalan Cisco Configuration Professional**

Cisco Configuration Professional (CCP) merupakan sebuah perangkat lunak berbasis Java, yang berfungsi untuk melakukan konfigurasi terhadap LAN, WAN, fitur keamanan yang terdapat pada router, serta beberapa komponen lain yang terdapat pada router. CCP dirancang untuk kebutuhan administrator jaringan kecil-hingga menengah, yang sudah memahami dasar-dasar jaringan.

CCP memberikan kemudahan dalam pengaturan jaringan Ethernet, WAN, firewall, dan VPN melalui *setup wizards*. Penggunaan Cisco SDM tidak membutuhkan keahlian dalam perangkat Cisco dan *Command-Line Interface* dari Cisco. Perangkat lunak ini dapat dipasang pada memori yang dimiliki oleh router, maupun komputer administrator yang mengatur router tersebut.

Pada router Cisco 1841, versi dari sistem operasi minimal yang dibutuhkan untuk menjalankan CCP adalah versi “12.3(8)T4”. Dan dengan pembaharuan yang telah dilakukan sebelumnya, dengan “c1841-advsecurityk9-mz.124-23.bin” yang merupakan versi 12.4, maka router tersebut sudah memenuhi standar SDM.

Pada router, CCP membutuhkan sekitar 6 MB memori untuk menampung seluruh data-data CCP. Sedangkan pada komputer yang digunakan untuk mengakses CCP, sistem minimum yang dibutuhkan adalah sebagai berikut:

- Sistem Operasi: Microsoft Windows XP Pro/2000 Pro SP4/ME/98/NT 4.0 SP4/Server 2003 Standard Edition
- Web Browser: Internet Explorer 5.5 / Netscape 7.1
- Java Runtime Environment (JRE) version 1.4.2\_05 / Java Virtual machine (JVM) 5.0.0.3810.

Pada dasarnya, untuk menginstal dan menjalankan CCP pada router, dan supaya router dapat berkomunikasi dengan komputer, dibutuhkan aktivasi terhadap http server dan telnet, yang merupakan platform dari CCP. Sehingga sebelum dapat menggunakan CCP, router tetap harus diakses melalui CLI menggunakan interface console. Langkah-langkahnya, adalah sebagai berikut:

1. Aktivasi HTTP dan HTTPS server pada router, dengan menggunakan perintah di bawah ini:

**Listing 4.18 Aktivasi HTTP dan HTTPS Server**

```

1 : R0# configure terminal
2 : Enter configuration commands, one per line. End with
   CNTL/Z
3 : R0(config)# ip http server
4 : R0(config)# ip http secure-server
5 : R0(config)# ip http authentication local
6 : R0(config)# ip http timeout-policy idle 600 life 86400
   requests 10000

```

2. Pembuatan sebuah user dengan privilege level 15, termasuk membuat username dan password untuk user tersebut dengan perintah “**username username privilege 15 secret 0 password**”. Username dan password tersebut, nantinya akan digunakan untuk login pada Cisco SDM.
3. Konfigurasi SSH dan Telnet untuk local login dan privilege level 15, dengan menggunakan perintah berikut ini:

**Listing 4.19 Konfigurasi SSH dan Telnet**

```

1 : R0(config)# line vty 0 4
2 : R0(config-line)# privilege level 15
3 : R0(config-line)# login local
4 : R0(config-line)# transport input telnet ssh
5 : R0(config-line)# exit

```

4. Mengaktifkan local logging untuk fungsi pengawasan (optional), dengan perintah “logging buffered 51200 warning”
5. Mengakhiri mode konfigurasi dengan perintah “end”

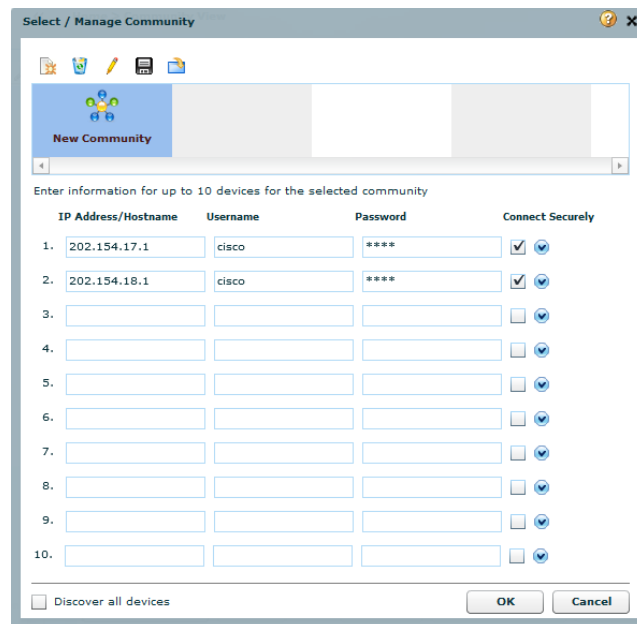
File-file yang dibutuhkan untuk menjalankan CCP dapat diunduh dari “<http://www.cisco.com/en/US/products/ps9422/index.html>”, dengan sebelumnya melakukan registrasi dan login ke situs tersebut.

CCP memanfaatkan komponen ActiveX yang terdapat pada Internet Explorer yang biasanya diblokir karena masalah keamanan. Oleh karena itu *blocker* yang terdapat Internet Explorer harus dimatikan.

Pada awal memulai CCP, aplikasi akan menampilkan sebuah interface “*Select / Manage Community*” yang meminta input alamat IP dari router yang akan dihubungkan menuju perangkat komputer yang bersangkutan. Adapun beberapa input yang diminta antara lain:

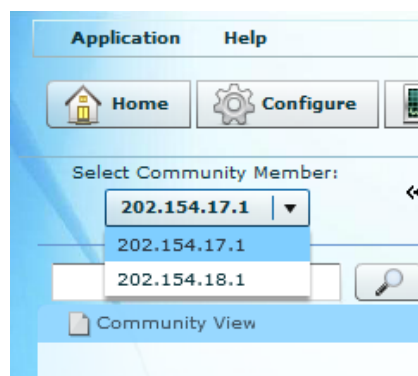
- IP address – alamat IP dari router
- Username – username dari telnet yang telah dikonfigurasi sebelumnya
- Password – password dari telnet yang telah dikonfigurasi sebelumnya
- Connect Securely – opsi untuk koneksi yang membutuhkan enkripsi
- Discover all devices – opsi untuk melakukan deteksi semua perangkat router yang sudah tercatat pada community.

Berbeda dengan Cisco SDM yang hanya mampu terhubung dengan sebuah perangkat pada satu sesi, CCP mampu terhubung dengan beberapa perangkat sekaligus. Adapun interface “Select / Manage Community” tersebut, dapat dilihat pada gambar 4.26 yang ada di bawah ini.



**Gambar 4.26**  
**Select / Manage Community**

Dalam operasinya, CCP mengakses router yang dimaksud dengan sebuah *selector* berbentuk *combobox* yang berdasarkan alamat IP maupun hostname yang dimiliki oleh router. Selector tersebut terdapat pada bagian kiri atas CCP.



**Gambar 4.27**  
**Select Community Member**

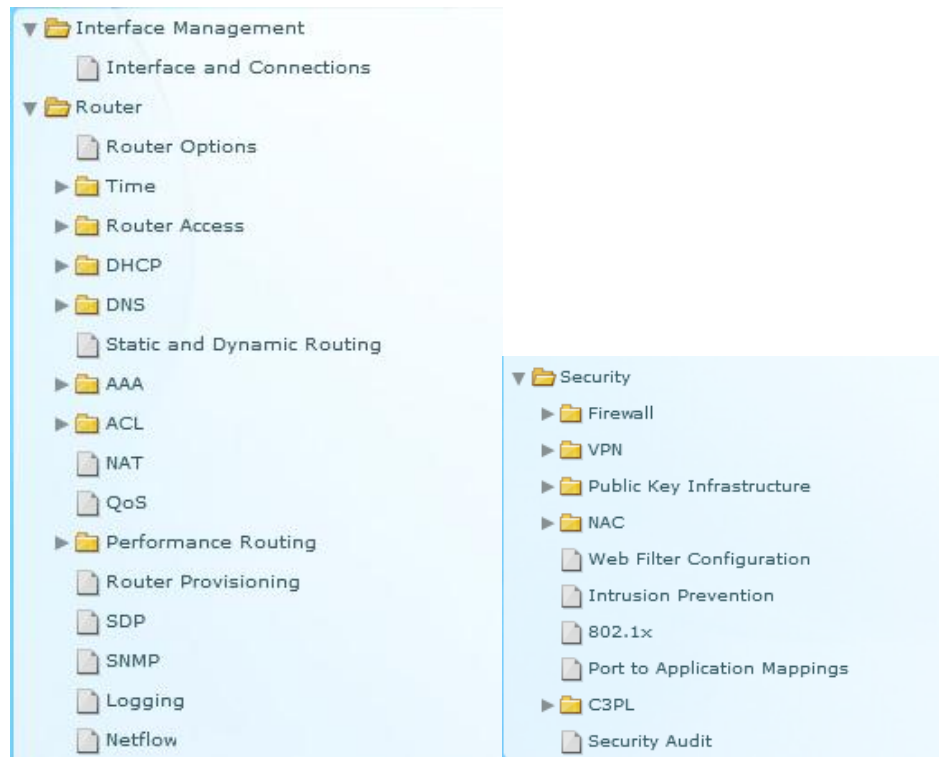
Terdapat tiga buah menu utama yang diwakili dengan tiga buah tombol pada jendela utama CCP, yakni Home, Configure, dan Monitor.



**Gambar 4.28**  
**Menu Utama CCP**

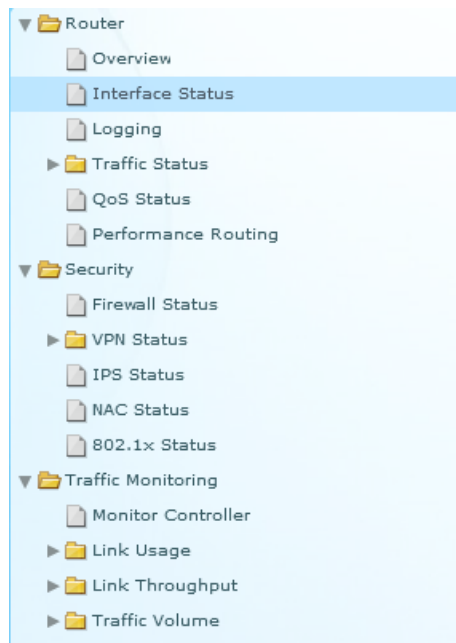
Menu home mengacu pada *Community View* di mana daftar perangkat router yang terdaftar sebelumnya ditampilkan. Configure mengacu pada menu konfigurasi router. Sedangkan monitor berfungsi untuk melakukan monitor atau pengawasan terhadap kondisi router.

Pada menu configure, terdapat beberapa komponen yang dapat diatur melalui CCP, yang terbagi dalam tiga bagian umum, yakni Interface Management, Router, dan Security. Berikut ini tampilan panel samping dari menu configure CCP.



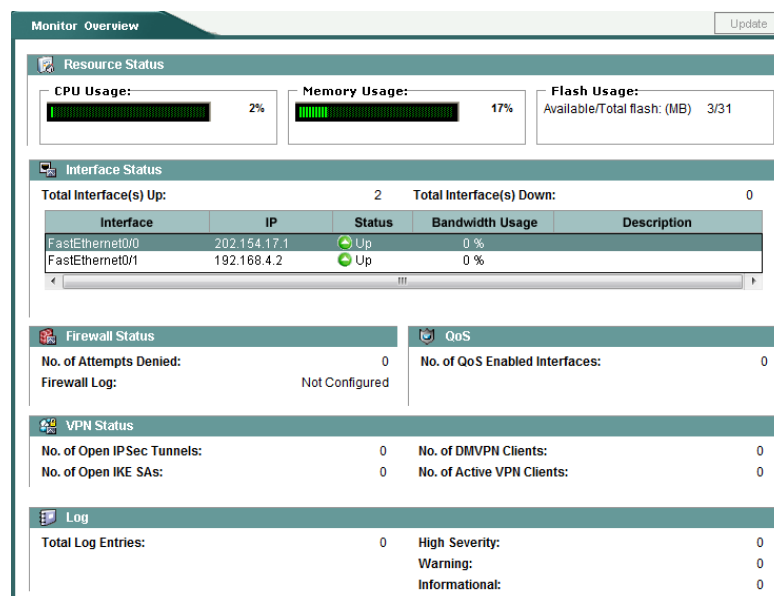
**Gambar 4.29**  
**Side Panel Configure CCP**

Demikian juga pada menu configure, yang terbagi menjadi tiga bagian umum. Panel samping monitor dapat dilihat pada gambar berikut ini.



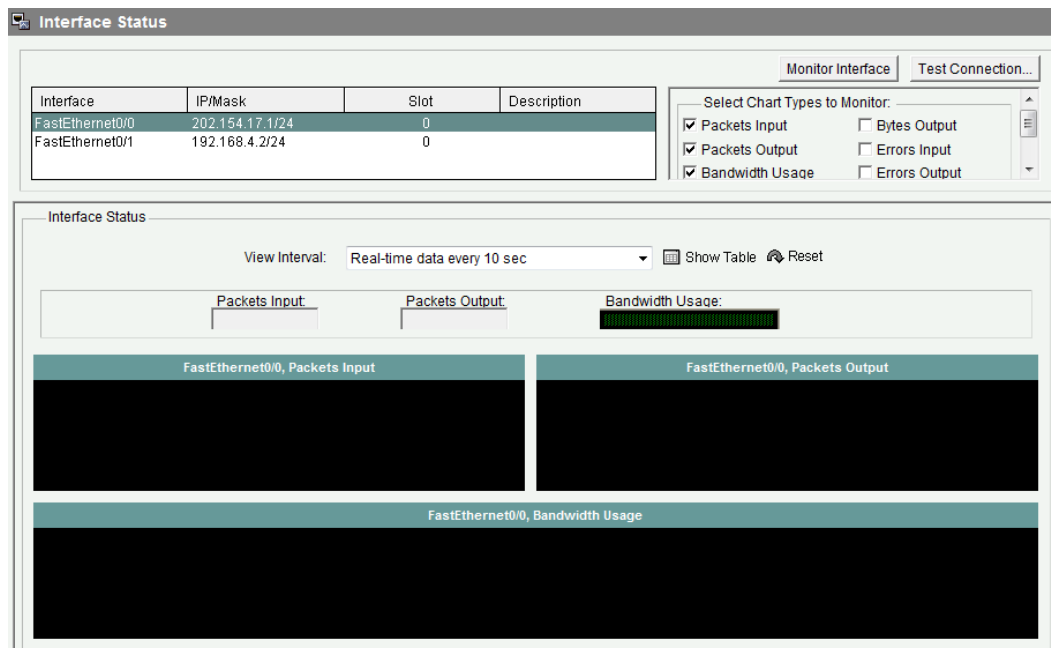
**Gambar 4.30**  
**Side Panel Monitor CCP**

Pada monitor overview, akan diperlihatkan status singkat dari beberapa komponen utama dari router seperti CPU, Memory, dan Interface.



**Gambar 4.31**  
**Overview Monitor CCP**

Selain itu, pada interface monitor juga ditampilkan status dari interface yang terpasang pada router.



**Gambar 4.32**  
**Interface Monitor CCP**

Pada interface status, ditampilkan juga statistik dari setiap interface, seperti packets input, packets output, dan bandwidth usage.

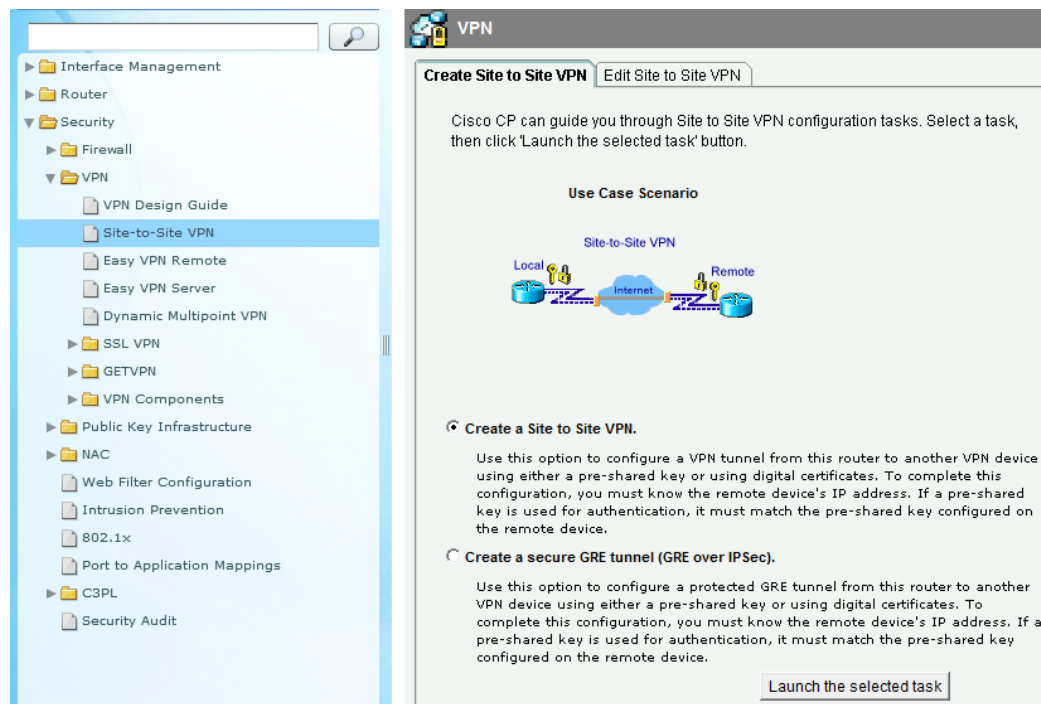
#### 4.5.2. VPN IPsec dengan Cisco Configuration Professional

CCP menyediakan setup wizard untuk melakukan konfigurasi terhadap komponen router. Baik pada hal mendasar seperti interface, maupun konfigurasi yang lebih mumpuni seperti security dan firewall. Setup wizard tersebut melakukan konversi terhadap input dari user, menjadi sebuah teks konfigurasi, dan kemudian mengirimkan konfigurasi tersebut menuju router yang dimaksud.

Demikian pula untuk membentuk VPN IPsec. Dengan menggunakan CCP, konfigurasi router, termasuk IKE proposal dan IPsec transform-set yang dibahas pada sub-bab sebelumnya, dapat dilakukan dengan mudah tanpa harus menghafal perintah-perintah pada CLI.



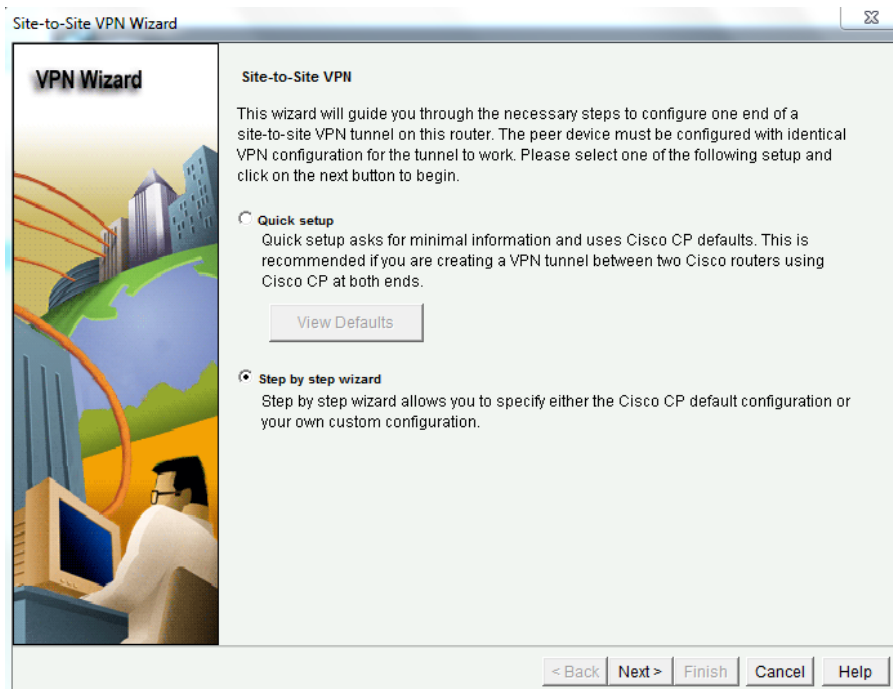
Untuk membentuk VPN IPsec, yang harus dituju adalah menu configure, security, dan site-to-site VPN. Kemudian memilih opsi “Create a Site to Site VPN” dan kemudian menekan tombol “Launch the selected task”. Adapun menu tersebut dapat dilihat pada gambar 4.33 berikut ini.



**Gambar 4.33**  
**Site-to-Site VPN Wizard**

Pada gambar tersebut terdapat sebuah opsi “Create a secure GRE tunnel (GRE over IPsec)”, opsi tersebut digunakan untuk membentuk tunnel GRE. Seperti pada pembahasan pada bab II, di mana GRE atau Generic Route Encapsulating hanya membungkus paket asal, tanpa melakukan enkripsi pada paket asalnya. Sehingga opsi tersebut hanya untuk tunneling saja tanpa enkripsi.

Setelah itu akan ditampilkan sebuah jendela yang memberikan dua buah pilihan setup, yakni quick setup dan step by step wizard. Opsi quick setup menawarkan proses setup yang cepat, sedangkan step by step wizard memberikan konfigurasi per langkah. Untuk kali ini, akan digunakan opsi step by step wizard untuk lebih memahami cara penggunaan CCP wizard untuk VPN. Gambar jendela tersebut dapat dilihat pada gambar 4.34 berikut ini.



**Gambar 4.34**  
**Step by Step Wizard**

Pada awal konfigurasi, CCP akan meminta beberapa input awal, antara lain:

- Interface for VPN connection – pemilihan interface mana yang akan digunakan sebagai jalur awal tunnel VPN. Detail dari interface yang bersangkutan dapat dilihat melalui tombol details yang ada di samping combobox interface.
- Jenis alamat IP dari remote peer – jenis alamat IP dari remote peer, dapat berupa IP static, maupun IP dynamic
- Alamat IP dari remote peer – diisi dengan alamat IP remote peer, apabila dipilih opsi IP static pada jenis alamat IP dari remote peer
- Autentikasi yang akan digunakan – terdapat dua jenis autentikasi pada setup wizard ini, yakni pre-shared keys dan digital certificates. Metode Rivest Shamil Adleman, termasuk ke dalam digital certificate.
- Pre-shared Keys – apabila digunakan pre-shared keys, maka harus diisi dengan preshare keys yang sama dengan remote peer

**VPN Connection Information**

Select the interface for this VPN connection: FastEthernet0/1 Details...

---

**Peer Identity**

Select the type of peer(s) used for this VPN connection: Peer with static IP address

Enter the IP address of the remote peer: 192.168.6.1

---

**Authentication**

Authentication ensures that each end of the VPN connection uses the same secret key.

☒ Pre-shared Keys ☐ Digital Certificates

pre-shared key: [masked]

Re-enter Key: [masked]

< Back Next > Finish Cancel Help

**Gambar 4.35**  
**Tahap Awal Site-to-Site VPN Wizard**

Kemudian, CCP akan meminta pemilihan Internet Key Exchange (IKE) policy. Terdapat default policy dengan konfigurasi sebagai berikut:

- Priority : 1
- Encryption : 3DES
- Hash : SHA-1
- DH Group : group 2
- Authentication: Pre-shared keys

Untuk menambahkan sebuah policy baru, dapat menggunakan tombol add. Berikut ini tampilan form “Add IKE Policy”.

**Add IKE Policy**

Configure IKE Policy

Priority: 10

Authentication: PRE\_SHARE

Encryption: AES\_256

D-H Group: group5

Hash: SHA\_1

Lifetime: 24 0 0 HH:MM:SS

OK Cancel Help

of the policies listed below.

and the Edit... button to edit an existing policy.

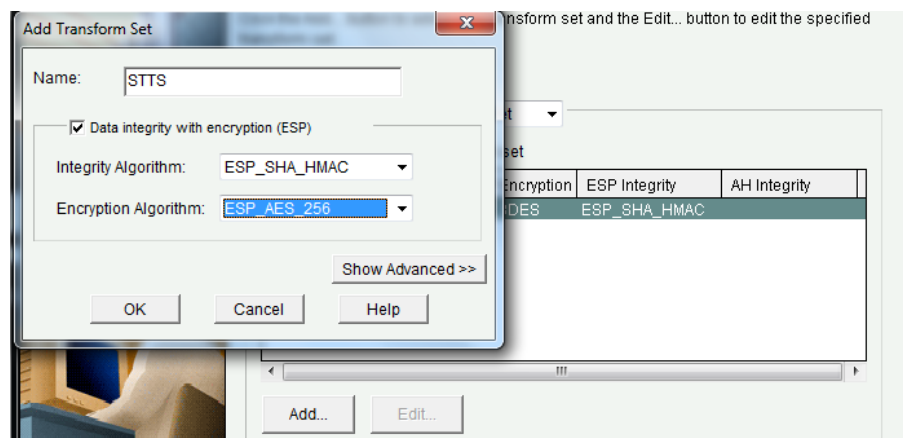
D-H Group	Authentication	Type
group2	PRE_SHARE	Cisco CP Defau

**Gambar 4.36**  
**IKE Policy Wizard**

Tahap selanjutnya adalah tahap penentuan IPsec transform set. Seperti IKE, terdapat default transform-set dengan detail sebagai berikut:

- Name : ESP-3DES-SHA
- Encryption : ESP\_3DES
- Integrity : ESP\_SHA\_HMAC

Untuk menambah sebuah transform-set baru, dapat menggunakan tombol add. Berikut ini tampilan dari form “transform-set”.



**Gambar 4.37**  
**Transform-set Wizard**

Langkah berikutnya adalah perlindungan jaringan. Proteksi ini bekerja dengan menggunakan firewall atau Access Control List (ACL). Input yang diminta adalah alamat IP dan subnet mask dari local network (source) dan remote network (destination), bukan alamat IP dari ujung-ujung tunnel VPN. Apabila digunakan konfigurasi Router 1 pada uji coba pada sub-bab sebelumnya, maka konfigurasi yang harus diinputkan adalah sebagai berikut:

- Local Network
  - IP Address : 202.154.17.0
  - Subnet Mask : 255.255.255.0
- Remote Network
  - IP Address : 202.154.18.0
  - Subnet Mask : 255.255.255.0

Apabila ACL sudah terdaftar pada konfigurasi route, maka dapat digunakan label dari ACL tersebut dengan memasukkannya pada opsi “Create / Select an access-list for IPsec traffic”. Konfigurasi dari ACL ini dapat dilihat pada gambar 4.38 berikut ini.

Protect all traffic between the following subnets

**Local Network**  
Enter the IP address and subnet mask of the network where IPsec traffic originates.  
IP Address: 202.154.17.0  
Subnet Mask: 255.255.255.0 or 24

**Remote Network**  
Enter the IP Address and Subnet Mask of the destination Network.  
IP Address: 202.154.18.0  
Subnet Mask: 255.255.255.0 or 24

Create/Select an access-list for IPsec traffic

**Gambar 4.38**  
**Access Controll List Wizard**

Dengan demikian, proses input telah selesai dilakukan, dan CCP akan menampilkan ringkasan dari konfigurasi yang sudah dilakukan sebelumnya. Contoh ringkasan tersebut, dapat dilihat pada gambar berikut ini.

Summary of the Configuration

Click Finish to deliver the configuration to the router.

Interface: FastEthernet0/1  
Peer Device: 192.168.6.1  
Authentication Type : Pre-shared key  
pre-shared key: \*\*\*\*\*

IKE Policies:

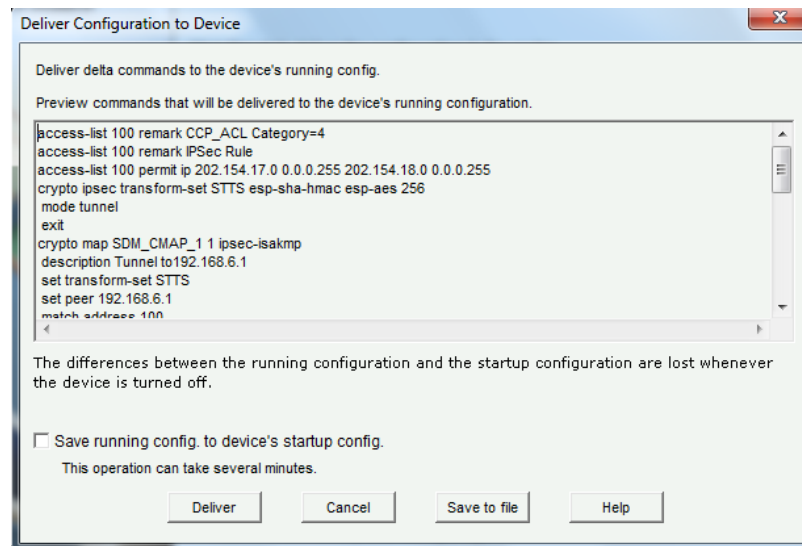
Hash	DH Group	Authentication	Encryption
SHA_1	group5	PRE_SHARE	AES_256
SHA_1	group2	PRE_SHARE	3DES

Transform Sets:  
Name: STTS  
ESP Encryption: ESP\_AES\_256  
ESP Integrity: ESP\_SHA\_HMAC  
Mode: TUNNEL

☐ Test VPN connectivity after configuring.

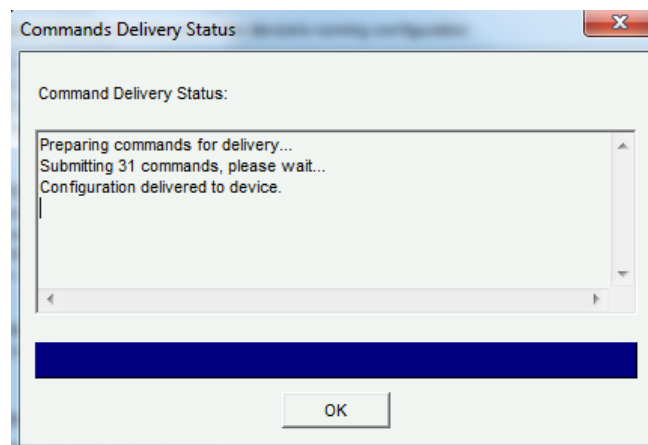
**Gambar 4.39**  
**Configuration Summary**

Setelah menerima konfirmasi persetujuan, CCP akan mengubah konfigurasi yang telah diterima tersebut, menjadi sebuah teks, yang akan meminta persetujuan untuk dikirimkan menuju router yang bersangkutan dengan menggunakan tombol “Deliver”.



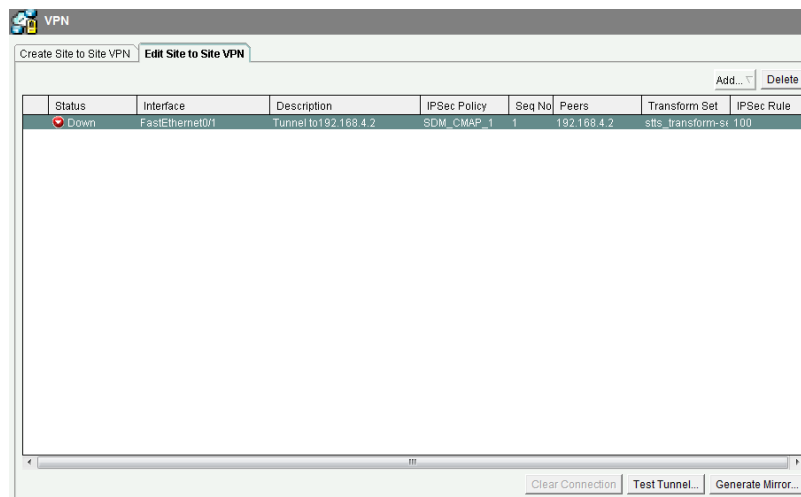
**Gambar 4.40**  
**Preview Commands**

Dengan tombol deliver, CCP akan mengirimkan perintah-perintah tersebut menuju running config dari router. Status pengiriman diperlihatkan dengan sebuah form yang dilengkapi dengan sebuah progress bar seperti pada gambar 4.41 di bawah ini.



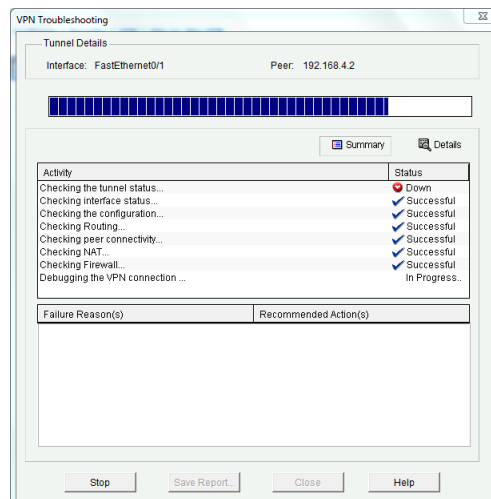
**Gambar 4.41**  
**Command Delivery Status**

Setelah kedua perangkat diatur konfigurasinya, maka harus dipastikan terbentuknya tunnel VPN yang telah dibuat. Kembali pada menu configure site-to-site VPN pada tab Edit site-to-site VPN, dapat dilihat status dari tunnel VPN. Apabila status menunjukkan “down”, maka tunnel belum terbentuk dengan sempurna, oleh karena itu harus dilakukan test tunnel untuk menguji koneksi, serta menemukan kesalahan bila terjadi kesalahan konfigurasi.



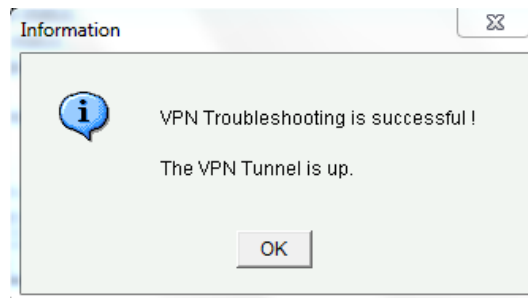
**Gambar 4.42**  
**VPN Status Down**

Dengan menggunakan test tunnel, maka akan terbuka sebuah jendela yang melakukan uji coba secara otomatis setelah ditekan tombol start.



**Gambar 4.43**  
**VPN Troubleshooting**

Jika tidak terjadi kesalahan, dan tunnel sudah terbentuk dengan sempurna, maka CCP akan memberikan konfirmasi seperti gambar 4.44 di bawah ini. Namun jika terjadi kesalahan, maka CCP akan memberikan solusi untuk menyempurnakan konfigurasi.



**Gambar 4.44**  
**VPN Tunnel Up**

Sehingga pada tab Edit site-to-site VPN sebelumnya, status akan berubah menjadi dari Down menjadi Up.

 The screenshot shows the 'VPN' configuration window with the 'Edit Site to Site VPN' tab selected. Below the tabs is a table with the following data:
 

Status	Interface	Description	IPSec Policy	Seq No	Peers	Transform Set	IPSec Rule
Up	FastEthernet0/1	Tunnel to 192.168.6.2	SDM_CMAP_1	1	192.168.6.2	ssts_transform-sr	100

**Gambar 4.45**  
**VPN Status Up**

#### 4.6. Kekurangan dan Kelebihan CCP

Berdasarkan uji coba CCP yang sudah dilakukan dalam membentuk VPN dengan menggunakan ADSL maupun tanpa ADSL, terdapat beberapa kekurangan dan kelebihan dalam CCP ini. Berikut ini kelebihan dari CCP:

- CCP mampu mempersingkat waktu pembentukan VPN IPsec, daripada dengan melakukan input manual pada CLI.
- Graphical User Interface dan Setup Wizard mempermudah user dalam menggunakan Router Cisco 1841.
- Terdapat fasilitas troubleshooting yang dapat membantu user dalam memeriksa kesalahan konfigurasi pada router.



- Terdapat beberapa fasilitas yang telah diperbaiki, yang sebelumnya tidak berjalan dengan sempurna pada Cisco SDM.
- Mampu terhubung dengan beberapa perangkat sekaligus.
- Telah mendukung modul-modul WIC yang tersedia.

Selain kelebihan pada CCP, terdapat beberapa kekurangan dari CCP yaitu adalah sebagai berikut:

- Masih menggunakan ActiveX yang rawan dengan malware.
- Masih belum mendukung JRE 1.7, versi Java maksimal yang dapat digunakan adalah JRE 1.6 update 35.
- Konfigurasi awal masih harus dilakukan melalui console, sehingga tidak dapat terlepas dari CLI dan console port.
- Beberapa fitur yang dimiliki oleh Router Cisco 1841 masih belum didukung oleh CCP sehingga harus dilakukan melalui CLI, seperti pembuatan VPDN dan interface dialer pada interface fast ethernet.