BAB III
IMPLEMENTASI DAN STUDI KASUS

Pada bab ini akan dibahas mengenai tahap-tahap implementasi VPN IPsec yang akan diaplikasikan pada jaringan laboratorium jaringan komputer STTS, dengan sebuah jaringan independen yang berada di luar jaringan STTS, yang disebut dengan Jaringan Remote.

3.1. Persiapan

Untuk membentuk sebuah jaringan VPN dalam pembahasan studi kasus ini, dibutuhkan beberapa komponen pendukung. Berikut ini komponen-komponen yang diperlukan untuk mendukung implementasi studi kasus ini:

- Router Cisco 1841 dengan Sistem Operasi "c1841-advsecurityk9-mz.124-23.bin"
- Koneksi Internet ADSL dengan IP publik statis

3.1.1. Router

Pada studi kasus ini, router merupakan komponen utama pembentuk jaringan VPN. Router bertindak sebagai gerbang atau gateway yang merupakan jalan keluar utama yang dilalui oleh semua paket data ketika akan keluar dari jaringannya. Dalam pokok bahasan ini, router dapat diibaratkan sebagai pintu masuk sebuah terowongan yang menghubungkan dua titik satu sama lain.

Dalam studi kasus ini, digunakan Router Cisco 1841 sebagai VPN gateway. Router ini merupakan salah satu seri dari Router Cisco 1800. Berikut ini merupakan beberapa fitur yang ditawarkan oleh router ini:

- Kemampuan kinerja WAN pada tingkat T1/E1
- Mendukung modularitas dengan lebih dari 90 modul yang tersedia
- Mendukung mayoritas WAN Interface Card (WIC), Voice/WAN Interface Card (VWICS), dan Voice Interface Card (VIC)
- Dua buah 10/100 Fast Ethernet Port

- Keamanan
  - Enkripsi On-board
  - Dukungan terhadap 800 tunnel VPN dengan Modul AIM
  - Proteksi antivirus melalui Network Admission Control (NAC)
  - Intrusion Prevention dan Cisco IOS Firewall

Gambar 3.1
Router Cisco 1841

Selain konektor sumber daya, Router Cisco 1841 ini memiliki beberapa interface yang dapat digunakan :

- Dua buah port fast ethernet

  Port ini digunakan untuk koneksi antar perangkat, baik switch, komputer, ataupun router yang lainnya dengan menggunakan kabel UTP dan konektor RJ45.
- Satu buah port console

  Port ini digunakan untuk menghubungkan router dengan perangkat komputer melalui kabel serial RS-232, yang berfungsi untuk melakukan konfigurasi terhadap router yang bersangkutan melalui Hyper Terminal.
- Satu buat port AUX

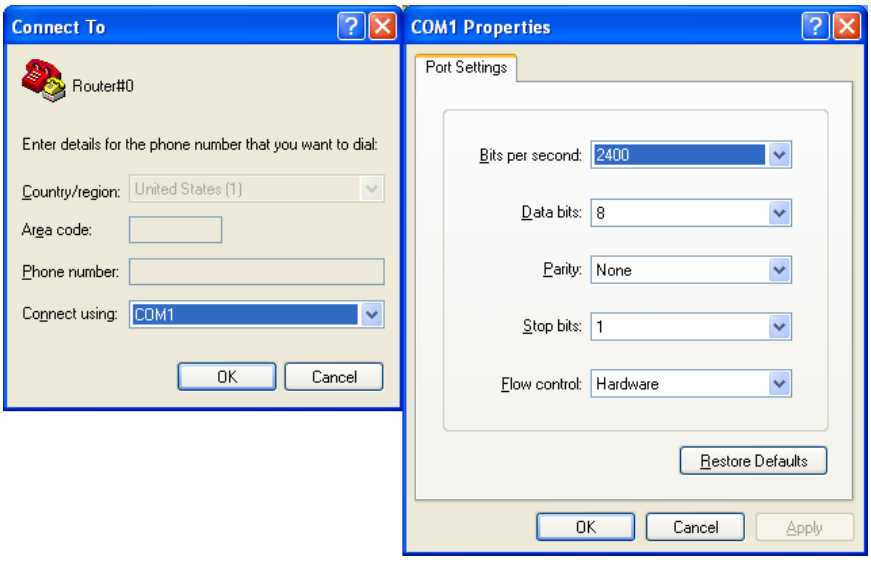
  Port ini berguna untuk menghubungkan router dengan modem eksternal, yang berfungsi sebagai koneksi cadangan untuk melakukan remote troubleshooting apabila koneksi pada jaringan utama terputus.

- Satu buah slot Compact Flash

  Slot ini berfungsi untuk memuat external compact flash memory yang berisi konfigurasi dan sistem operasi dari router. Konfigurasi ini dibaca pada saat router melakukan booting. Ukuran data dari compact flash bervariasi, 32MB, 64MB, dan 128MB.
- Satu buah port USB 1.1

  Port ini dapat digunakan untuk pendistribusian parameter-parameter yang diperlukan dalam pengaturan router, seperti pendistribusian public key, dan pendistribusian credential yang dibutuhkan dalam pembentukan SSL.
- Dua buah slot modular

  Slot ini dapat diisi dengan beberapa modul Cisco yang dijual terpisah dari perangkat router yang bersangkutan. Adapun beberapa modul yang tersedia, antara lain Ethernet Switch, Wireless LAN, Serial WAN Interface, ADSL, dan beberapa modul WAN lainnya.



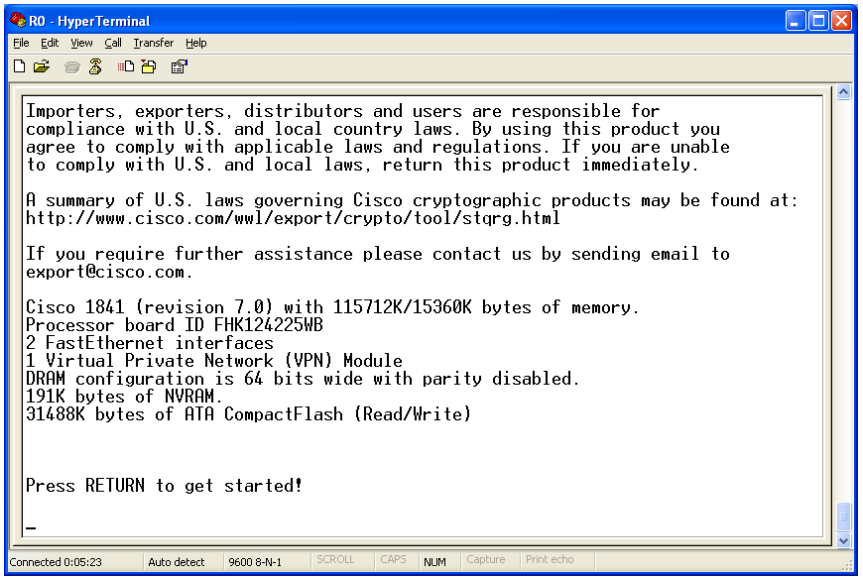
Gambar 3.2
Konfigurasi Hyper Terminal

Pengaturan konfigurasi router ini dilakukan menyambungkan kabel console pada port console yang terletak pada router, dan ujung lainnya pada port serial komputer. Untuk mengakses port serial tersebut, digunakan Hyper Terminal

dengan menghubungkan Hyper Terminal pada “COM1” dan konfigurasi port setting sebagai berikut:

- Bits per second : 9600
- Data bits : 8
- Parity : None
- Stop bits : 1
- Flow controll : None

Tampilan yang diperlihatkan pada Hyper Terminal hanya berupa tampilan command line, seperti tampilan command prompt pada Windows. Pada konfigurasi awal saat router dinyalakan, akan ditampilkan informasi tentang versi sistem operasi yang digunakan oleh router tersebut. Setelah itu router akan menampilkan beberapa tahapan bootingnya, termasuk identifikasi interface yang dimiliki oleh router tersebut dan memori yang digunakan. Hingga pada akhirnya router akan meminta input untuk memasukkan initial configuration. Karena konfigurasi akan dimasukkan secara manual, maka dapat dipilih “no”. Setelah muncul tulisan “Press RETURN to get started”, maka saat itu router tersebut siap dikonfigurasi.



Gambar 3.3
Hyper Terminal

Selain melalui koneksi serial dengan interface Hyper Terminal, konfigurasi router juga dapat dilakukan melalui interface fast ethernet melalui telnet, yang interfacenya tidak jauh berbeda dengan Hyper Terminal. Untuk melakukan koneksi melalui telnet, terdapat beberapa pengaturan yang harus dilakukan pada router, seperti pembuatan username dan password dengan privilege level 15. Selain itu, interface fast ethernet juga haru diaktifkan dan diberi alamat IP. Adapun konfigurasi tersebut dapat dilihat pada listing berikut ini.

Listing 3.1 Konfigurasi SSH dan Telnet

```
1 :   R0(config)# username cisco privilege 15 secret 0 stts
2 :   R0(config)# line vty 0 4
3 :   R0(config-line)# privilege level 15
4 :   R0(config-line)# login local
5 :   R0(config-line)# transport input telnet ssh
6 :   R0(config-line)# exit
7 :   R0(config)# interface fastethernet0/0
8 :   R0(config-if)# ip address 192.168.1.1 255.255.255.0
9 :   R0(config-if)# no shutdown
```

Sistem operasi dari router ini tersimpan pada external compact flash yang terpasang pada slot yang sudah tersedia. Sistem operasi standar yang diberikan oleh Cisco pada router ini adalah "c1841-ipbase-mz.124-1c.bin". akan tetapi, sistem operasi tersebut belum mendukung VPN. Untuk itu Cisco telah menyediakan beberapa versi IOS lainnya sesuai dengan kebutuhan. Untuk modul VPN, Cisco menyediakan beberapa IOS yang akan dijabarkan pada tabel di berikut ini:

Tabel 3.1
Jenis-Jenis Cisco IOS

Feature Set	Image	VPN
IP Base	c1841-ipbase-mz	x
IP Voice	c1841-ipvoice-mz	x
Enterprise base	c1841-entbase-mz	v
Advance Security	c1841-advsecurityk9-mz	v
SP Services	c1841-spservicesk9-mz	v
Enterprise Services	c1841-entservicesk9-mz	v
Advanced IP Services	c1841-advipservicesk9-mz	v
Advaced Ent. Services	c1841-adventerprisek9-mz	v

Sesuai dengan kebutuhan tugas akhir ini, maka sistem operasi yang ada akan diperbarui menjadi "c1841-advsecurityk9-mz.124-23.bin". Sistem operasi ini dipilih karena kebutuhan minimal pengoperasiannya dipenuhi oleh Router 1841 yang ada. Selain itu, sistem operasi ini merupakan salah satu varian dari Advance Security, yang memiliki fungsionalitas keamanan yang dibutuhkan dalam pembangunan VPN.

Untuk melakukan pembaharuan sistem operasi ini, dibutuhkan bantuan dari sebuah aplikasi TFTP Server. Dalam tugas akhir ini akan digunakan aplikasi TFTP Server bernama Tftpd32. Adapun tahap-tahap yang harus dilakukan untuk melakukan pembaharuan sistem operasi IOS adalah sebagai berikut:

1. Proses back up data sistem operasi IOS yang sedang terpasang pada router. Proses ini dapat dilakukan dengan menghubungkan interface fast ethernet 0/0 router dengan komputer, IP router dan komputer diatur ke dalam satu jaringan dan TFTP Server dijalankan. Dengan mengetikkan perintah "show flash", flash memory dapat diketahui, termasuk file IOS yang sedang terpasang. Proses back up diawali dengan memasukkan perintah "copy flash tftp". Sesudah itu, router akan meminta input source filename, alamat IP TFTP Server, dan destination filename. Backup ini bertujuan supaya file asal tetap tersimpan dan dapat digunakan kembali apabila file yang baru mengalami masalah.

Listing 3.2 Back Up IOS Menuju TFTP Server

```
1 :   R0#show flash:
2 :   System flash directory:
3 :   File  Length   Name/status
4 :     3   33591768 c1841-ipbase-mz.124-1c.bin
5 :     2   28282    sigdef-category.xml
6 :     1   227537   sigdef-default.xml
7 :   [33847587 bytes used, 30168797 available, 64016384
      total]
8 :   63488K bytes of processor board System flash
      (Read/Write)
9 :   R0#copy flash: tftp
10 :  Source filename []?c1841-ipbase-mz.124-1c.bin
11 :  Address or name of remote host []? 192.168.1.1
12 :  Destination filename [c1841-ipbase-mz.124-1c.bin]?
```

2. Sesudah back up dilakukan, maka data pada router bisa dihapus dengan perintah "delete flash: c1841-ipbase-mz.124-1c.bin", lalu reboot router dengan perintah "reload".

Listing 3.3 Delete IOS

```
1 :   R0# delete flash: c1841-ipbase-mz.124-1c.bin
2 :   Delete filename [c1841-ipbase-mz.124-1c.bin]?
3 :   R0# reload
4 :   Proceed with reload? [confirm]
```

3. Karena tidak ada sistem operasi yang tersimpan pada flash memory, maka router akan masuk mode rommon. Sebelumnya persiapkan file "c1841-advsecurityk9-mz.124-23.bin" pada direktori TFTP Server. Pada rommon masukkan beberapa parameter-parameter di bawah ini, dan kemudian jalankan "tftpdnld":
   - IP_ADDRESS – alamat IP dari interface fast ethernet 0/0 router.
   - IP_SUBNET_MASK – subnet mask dari interface fast ethernet 0/0 router.
   - DEFAULT_GATEWAY – default gateway apabila server terletak di luar jaringan router (optional).
   - TFTP_SERVER – alamat IP dari TFTP Server yang menyediakan file, dalam hal ini komputer.
   - TFTP_FILE – nama file yang akan diunduh menuju router.

Listing 3.4 TFTPDNLD

```
1 :   rommon 1 > IP_ADDRESS=192.168.1.1
2 :   rommon 2 > IP_SUBNET_MASK=255.255.255.0
3 :   rommon 3 > DEFAULT_GATEWAY=192.168.1.254
4 :   rommon 4 > TFTP_SERVER=192.168.1.10
5 :   rommon 5 > TFTP_FILE=c1841-advsecurityk9-mz.124-23.bin
6 :   rommon 6 > set
7 :   DEFAULT_GATEWAY=192.168.1.254
8 :   IP_ADDRESS=192.168.1.1
9 :   IP_SUBNET_MASK=255.255.255.0
10 :  TFTP_FILE=c1841-advsecurityk9-mz.124-23.bin
11 :  TFTP_SERVER=192.168.1.10
12 :  rommon 7 > tftpdnld
```

4. Dan bila semua input dan koneksi tidak bermasalah, router akan mengunduh file tersebut secara otomatis. Setelah selesai perintahkan router untuk melakukan booting dengan perintah “boot”. Dan router akan melakukan booting dengan sistem operasi yang baru.

Dengan demikian, router telah siap dipergunakan untuk membangun sebuah jaringan VPN. Konfigurasi VPN sendiri akan dibahas pada sub-bab berikutnya.

3.1.2. Koneksi Internet ADSL

Saat ini biaya yang dibutuhkan untuk memperoleh layanan Internet sudah sangat terjangkau bagi masyarakat. Salah satu pilihan untuk koneksi internet adalah dengan menggunakan teknologi *Asymmetric Digital Subscriber Line* (*ADSL*). ADSL merupakan sebuah teknologi komunikasi data yang memungkinkan transmisi data dengan bandwith yang cukup besar melalui saluran kabel telepon, dan lebih cepat daripada kecepatan yang mampu diberikan oleh modem dial up 56k.

Kecepatan tersebut diperoleh melalui pemanfaatan frekuensi yang tidak digunakan oleh jaringan telepon. Sebuah *splitter* atau *DSL filter*, memungkinkan sebuah jalur telepon untuk digunakan oleh layanan telepon dan ADSL secara bersamaan.

Di Indonesia sendiri, saat ini layanan ADSL yang paling banyak digunakan adalah layanan ADSL dari Telkom Speedy, yang harganya relatif terjangkau, baik bagi perorangan maupun perusahaan sesuai dengan kebutuhan kapasitas bandwith yang dikehendaki.

Pengguna layanan ADSL memerlukan sebuah ADSL Router untuk memperoleh layanan dari provider. Adapun beberapa konfigurasi WAN ADSL Router D-Link DSL-526B untuk layanan Telkom Speedy adalah sebagai berikut:

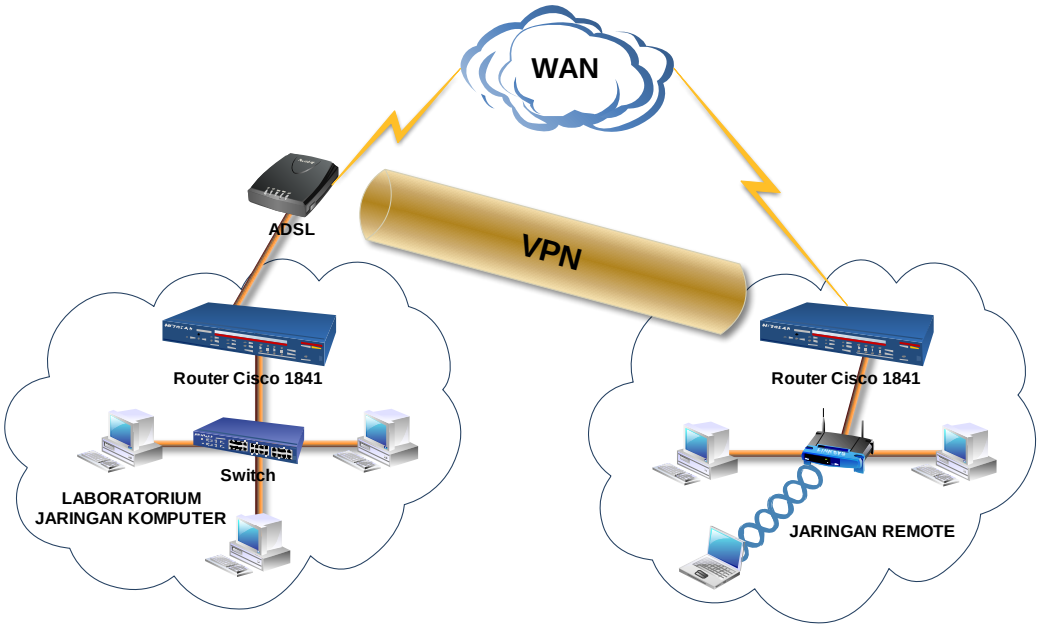
- Port/VPI/VCI : 0/0/35
- Connection Type : PPPoE

- Service Name : pppoe_0_0_35_1_Speedy
- Service Category : UBR
- IP Address : Automatically Signed
- Service State : Enabled
- NAT : Enabled
- Firewall : Enabled
- IGMP Multicast : Disabled
- Quality of Service : Enabled

Selain menggunakan router ADSL D-Link DSL-526B ini, banyak beberapa router ADSL dari beberapa merek yang lainnya yang dipakai. Harga router ADSL cukup terjangkau bagi kalangan publik.

3.2. Implementasi

Dalam tugas akhir ini, akan diimplementasikan sebuah jaringan VPN yang menghubungkan Laboratorium Jaringan Komputer dengan Jaringan Remote. Di mana kedua jaringan tersebut memilik privasi, dalam komunikasinya melalui jaringan publik. Adapun konfigurasi jaringannya tergambar pada gambar 3.7.



Gambar 3.4
Jaringan VPN yang Akan Dibuat

Terdapat tiga buah metode yang dapat digunakan dalam studi kasus ini, antara lain:

- RFC 1483 Bridged

  Metode ini lebih dikenal dengan nama bridging. Metode ini mengakibatkan alamat IP publik yang diperoleh dari ISP, terpasang pada perangkat yang melakukan dial up. Perangkat tersebut dapat berupa router, maupun komputer. Sedangkan router hanya bertindak sebagai fasilitator saja, dan hanya memiliki alamat IP privat sebagai penghubungnya dengan perangkat pelaku dial up.

- Port Forwarding

  Konsep dari port forwarding adalah melakukan pemetaan terhadap port request. Di mana alamat IP tetap dimiliki oleh Router ADSL. Pemetaan dilakukan dengan sebelumnya mengisi tabel port forwarding yang terdapat pada Router ADSL. Misalnya request terhadap port 80, diarahkan menuju komputer dengan IP privat 192.168.101.50. Penggunaan metode port forwarding ini

- Penambahan modul ADSL pada Router Cisco 1841

  Metode ini merupakan pilihan terakhir pada implementasi ini. Yaitu dengan menambahkan sebuah modul WIC-1ADSL, yang dipasangkan pada slot WIC yang tersedia pada Router Cisco 1841. Dengan modul ini, router dapat secara langsung melakukan dial-up menuju ISP, dan secara langsung menerima IP publik yang diberikan oleh ISP.

Gambar 3.5
Modul WIC-1ADSL

Pada studi kasus ini, akan digunakan dua metode dalam penggunaan koneksi ADSL, yaitu RFC 1483 Briged dan penambahan modul ADSL. Router Cisco 1841 pada Laboratorium Jaringan Komputer, akan menggunakan metode RFC 1483 Briged. Sedangkan pada Jaringan Remote, akan menggunakan Router Cisco 1841 dengan menggunakan modul WIC-1ADSL.

Dalam implementasi ini, penggunaan IP publik membutuhkan prioritas yang cukup besar. Di mana IP publik ini merupakan acuan bagi kedua router yang bertindak sebagai gateway VPN dalam mengirimkan paket data yang terenkripsi.

Dari beberapa protokol VPN yang ada, dalam implementasi ini lebih dipilih protokol IPSec. IPSec dipilih karena memiliki sebuah framework keamanan yang dapat dimodifikasi sesuai dengan kebutuhan keamanan yang diinginkan. Selain itu, penerapan IPSec juga lebih mudah dibanding protokol yang lainnya, serta mendukung semua mode yang ada.

Berdasarkan analisa yang telah dilakukan pada paragraf-paragraf sebelumnya, maka konfigurasi VPN pada router Cisco 1841 dapat dimulai. Pada skenario ini akan digunakan parameter-parameter IPSec sebagai berikut:

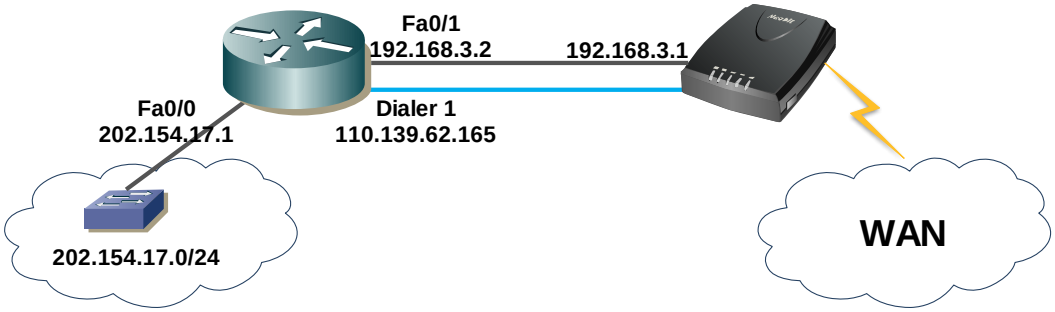
- Authentication: Pre-shared key
- Confidentiality: Advanced Encryption Standard 256 bits
- Integrity: Message Digest 5
- Diffie-Hellman: Group 5

3.2.1. Jaringan Laboratorium Jaringan Komputer

Jaringan Laboratorium Jaringan Komputer memiliki sebuah line dengan alamat IP 192.168.9.50/24, yang terhubung langsung dengan jaringan server STTS. Server ini, mampu melakukan by pass menuju router ADSL tanpa harus melewati router STTS.

Pada jaringan ini, sebuah Router Cisco 1841 terhubung dengan Router ADSL melalui interface Fast Ethernet 0/1 yang dimiliki oleh Router Cisco 1841. Sedangkan interface Fast Ethernet 0/0, terhubung pada sebuah switch yang menghubungkan router dengan komputer client.

Interface Fast Ethernet 0/0 dari Router Cisco 1841 memiliki alamat IP 202.154.17.1/24, dan bertindak sebagai gateway dari jaringan 202.154.17.0/24. Sedangkan interface Fast Ethernet 0/1 didefinisikan sebagai WAN Interface, yang memiliki alamat IP 192.168.3.2 yang terhubung dengan Router ADSL D-Link DSL-526B yang memiliki alamat IP 192.168.3.1. Kemudian IP publik nantinya akan terpasang pada interface Dialer 1 pada Router Cisco 1841.



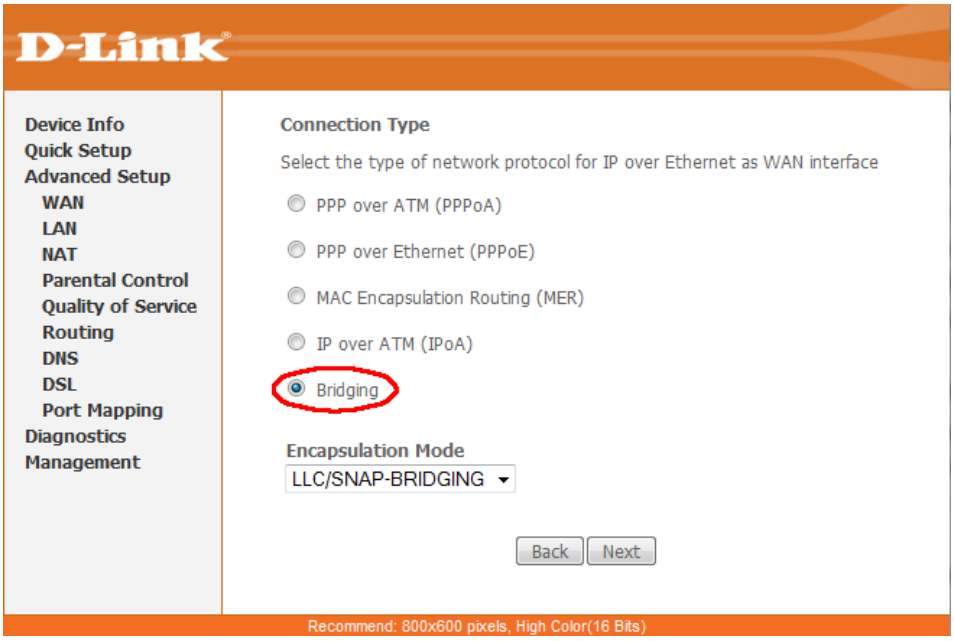
Gambar 3.6
RFC 1483 Bridge

Interface Dialer 1 ini dibentuk manual secara virtual pada interface Fast Ethernet 0/1 yang sebelumnya didefinisikan sebagai WAN interface. Interface Dialer ini bertugas untuk melakukan dial-up berdasarkan credential yang disediakan oleh ISP. Sehingga secara tidak langsung, Interface Fast Ethernet 0/1 memiliki 2 buah IP address, yakni IP Private, dan IP Publik. Dalam studi kasus ini, IP publik yang dimiliki oleh Interface Dialer 1 adalah 110.139.62.165.

Jaringan ini akan menggunakan metode bridging dalam koneksi ADSL. Sehingga yang melakukan dial up adalah Router Cisco 1841, dan router ADSL hanya bertindak sebagai fasilitator saja. Oleh karena itu, metode koneksi ADSL pada router ADSL harus diubah menjadi mode bridge.

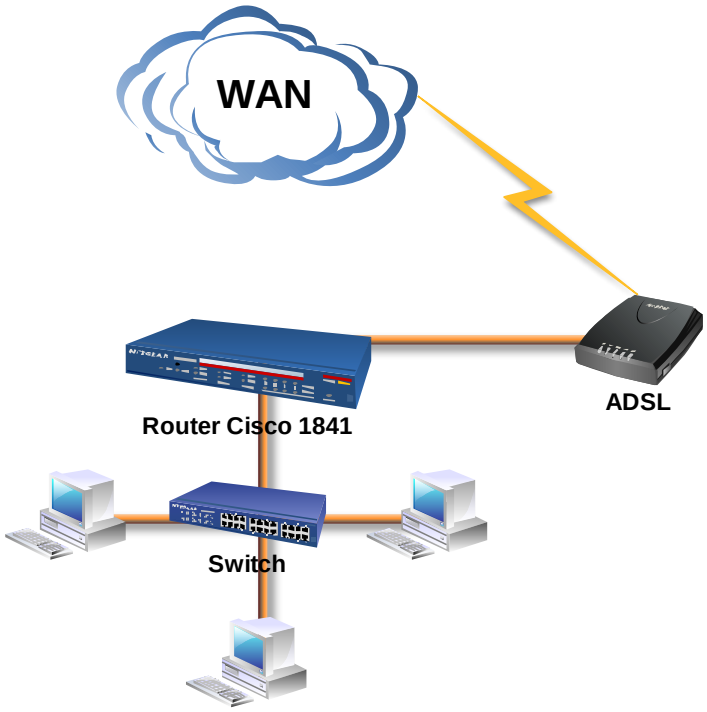
Dengan demikian, supaya sub jaringan di bawah router dapat berhubungan dengan Internet, maka juga router harus memiliki manajemen Network Address Translation tersendiri. Pada bahasan ini nantinya, akan digunakan metode Network Address Translation Overload.

Berikut ini tampilan interface modem ADSL D-Link DSL-526B jika diakses melalui browser.



Gambar 3.7
Mode Bridge pada D-Link ADSL

Ilustrasi jaringan Laboratorium Jaringan Komputer dapat dilihat pada gambar di bawah ini.



Gambar 3.8
Jaringan Laboratorium Jaringan Komputer

Setelah router ADSL diatur ke dalam mode bridge, maka Router Cisco 1841 harus dikonfigurasi pada kedua interface Fast Ethernet yang dimiliki. Interface Fast Ethernet 0/0 digunakan untuk jaringan lokal, sedangkan interface Fast Ethernet 0/1 diatur agar dapat melakukan dial up. Proses dial up merupakan proses request menuju ISP. Adapun konfigurasi selengkapnya adalah sebagai berikut.

1. Konfigurasi alamat IP Fast Ethernet 0/0

   Interface ini berfungsi sebagai interface yang terhubung pada jaringan lokal pada Router 1.

   Listing 3.5 Konfigurasi Alamat IP Fa0/0 Router 1

```
1 :   R1# configure terminal
2 :   Enter configuration commands, one per line.  End with
      CNTL/Z.
3 :   R1(config)# interface fast ethernet 0/0
4 :   R1(config-if)# ip address 202.154.17.0 255.255.255.0
5 :   R1(config-if)# no shutdown
6 :   R1(config-if)# end
7 :   R1#
```

2. Pembuatan Virtual Private Dialer Network

   Untuk membentuk sebuah interface yang mampu melakukan dial-up, dibutuhkan sebuah Virtual Private Diale Network (VPDN) yang diaplikasikan pada sebuah interface. Berikut ini konfigurasi VPDN.

   Listing 3.6 Konfigurasi VPDN Router 1

```
1 :   R1# configure terminal
2 :   Enter configuration commands, one per line.  End with
      CNTL/Z.
3 :   R1(config)# vpdn enable
4 :   R1(config)# vpdn-group 1
5 :   R1(config-vpdn)# request-dialin
6 :   R1(config-vpdn-req-in)# protocol pppoe
7 :   R1(config-vpdn-req-in)# exit
```

3. Konfigurasi Interface Fast Ethernet 0/1 sebagai interface WAN

   Konfigurasi terhadap interface Fast Ethernet 0/1 dilakukan agar interface tersebut dapat membentuk koneksi dengan ISP.

   Listing 3.7 Konfigurasi Fa0/1 Router1

```
1 :   R1# configure terminal
2 :   Enter configuration commands, one per line.  End with
      CNTL/Z.
3 :   R1(config)# interface fast ethernet 0/1
```

Listing 3.7 Konfigurasi Fa0/1 Router1 (Lanjutan)

```
4 :   R1(config-if)# description ADSL WAN Interface
5 :   R1(config-if)# ip address 192.168.3.2 255.255.255.0
6 :   R1(config-if)# no ip redirects
7 :   R1(config-if)# no ip unreachables
8 :   R1(config-if)# no ip proxy-arp
9 :   R1(config-if)# no ip mroute-cache
10 :  R1(config-if)# pppoe enable
11 :  R1(config-if)# pppoe-client dial-pool-number 1
12 :  R1(config-if)# no cdp enable
13 :  R1(config-if)# exit
```

4. Konfigurasi Interface Dialer

Interface dialer muncul saat VPDN terbentuk. Konfigurasi yang harus dilakukan adalah sebagai berikut.

Listing 3.8 Konfigurasi Interface Dialer Router1

```
1 :   R1# configure terminal
2 :   Enter configuration commands, one per line.  End with
      CNTL/Z.
3 :   R1(config)# interface dialer 1
4 :   R1(config-if)# description ADSL WAN Dialer
5 :   R1(config-if)# ip address negotiated
6 :   R1(config-if)# ip mtu 1492
7 :   R1(config-if)# ip nat outside
8 :   R1(config-if)# encapsulation ppp
9 :   R1(config-if)# no ip mroute-cache
10 :  R1(config-if)# dialer pool 1
11 :  R1(config-if)# dialer-group 1
12 :  R1(config-if)# no cdp enable
```

5. Konfigurasi Credential dari ISP

Credential yang dimaksud adalah username dan password yang diberikan oleh ISP. Pada mode PPPoE, credential ini terletak pada Router ADSL. Namun pada mode bridge, khusunya kasus ini, credential terletak pada Router Cisco 1841. Untuk Router 1, username isp adalah "152320204***@telkom.net", dan password isp "tdkqtn****"

Listing 3.9 Konfigurasi Credential Dialer Router1

```
1 :   R1(config-if)# ppp authentication chap pap callin
2 :   R1(config-if)# ppp chap hostname
      152320204***@telkom.net
3 :   R1(config-if)# ppp chap password 0 *r***d**r*
4 :   R1(config-if)# ppp pap sent-username
      152320204***@telkom.net password 0 *r***d**r*
5 :   R1(config-if)# exit
6 :   R1(config-if)# dialer-list 1 protocol ip permit
```

6. Konfigurasi Routing Protocol

   Routing Protocol berfungsi untuk membentuk tabel routing, yang nantinya tabel routing yang telah dibentuk tersebut, digunakan untuk mengarahkan paket yang singgah pada router tersebut. Terdapat beberapa jenis routing protocol yang dapat digunakan seperti Static Routing, RIP, OSPF, dan EIGRP. Dalam skenario ini, akan digunakan default route dengan metode static routing. Default route pada bahasan ini, diarahkan menuju WAN Interface, yakni Dialer 1. Konfigurasi default route dalam CLI dapat dilihat pada listing berikut ini.

   Listing 3.10 Konfigurasi Default Route

```
1 :   R1# configure terminal
2 :   R1(config)# ip route 0.0.0.0 0.0.0.0 Dialer1
```

7. Konfigurasi Access List

   Konfigurasi ini berfungsi untuk membuka ijin jalan pada interface Dialer. Konfigurasinya dapat dilihat seperti listing di bawah ini.

   Listing 3.11 Konfigurasi Access List

```
1 :   R1(config)# access-list 1 permit any
2 :   R1(config)# dialer-list 1 protocol ip permit
```

8. Konfigurasi Network Address Translation (NAT)

   NAT berfungsi untuk memetakan paket data yang keluar dari gateway, agar dapat kembali ke pengirim asal. Konfigurasi NAT dapat dilihat pada listing berikut ini.

   Listing 3.12 Konfigurasi NAT

```
1 :   R1# configure terminal
2 :   R1(config)# ip nat inside source list NAT interface
      dialer1 overload
```

9. Pembentukan IKE Policies

   IKE policies bertugas untuk mengendalikan autentikasi, algoritma enkripsi, serta metode petukaran kunci atau key exchange yang digunakan untuk membentuk peroposal IKE yang dikirimkan menuju titik akhir IPSec. Adapun tahapan konfigurasi IKE adalah sebagai berikut:

Listing 3.13 Konfigurasi IKE Router 1

```
1 :   R1# configure terminal
2 :   R1(config)# crypto isakmp enable
3 :   R1(config)# crypto isakmp policy 10
4 :   R1(config-isakmp)# authentication pre-share
5 :   R1(config-isakmp)# encryption aes 256
6 :   R1(config-isakmp)# hash md5
7 :   R1(config-isakmp)# group 5
8 :   R1(config-isakmp)# lifetime 3600
```

10. Konfigurasi Pre-shared Key

    Karena parameter autentikasi menggunakan pre-shared key, maka key atau kunci yang akan digunakan pada kedua router harus dikonfigurasi secara manual. Dalam skenario ini, digunakan key "cisco". Selain key, alamat IP dari router ujung juga harus dimasukkan. Dalam skenario ini, router ujung memiliki alamat IP "125.164.4.31".

    Listing 3.14 Konfigurasi Pre-Shared Key Router 1

```
1 :   R1(config)# crypto isakmp key cisco address
      125.164.4.31
```

11. Konfigurasi IPSec Transform Set

    IPSec Transform Set merupakan sekumpulan metode transformasi yang nantinya akan digunakan untuk proses enkripsi dan dekripsi dalam komunikasi jaringan VPN. Dalam studi kasus ini digunakan enkripsi AES dengan key 256-bit dan hash MD5.

    Listing 3.15 Konfigurasi IPSec Transform Set Router 1

```
1 :   R1(config)# crypto ipsec transform-set 50 esp-aes 256
      esp-md5-hmac
2 :   R1(cfg-crypto-trans)# exit
```

12. Pendefinisian jalur khusus pada ACL

    Tujuan utama pendefinisian ini adalah untuk memberikan akses paket dari kedua ujung gateway untuk melewati firewall pada router, di mana jalur di antara kedua router tersebut mengalami enkripsi.

    Listing 3.16 Konfigurasi ACL Router 1

```
1 :   R1(config)# access-list permit ip 202.154.17.0
      0.0.0.255 202.154.18.0 0.0.0.255
2 :   R1(config)# exit
```

13. Pembuatan dan Aplikasi Crypto Map

    Tugas utama crypto map adalah untuk melakukan verifikasi terhadap parameter-parameter kriptografi dari router gateway VPN di sisi yang lain. Dan memasangkan transform-set pada interface yang bersangkutan.

Listing 3.17 Pembuatan dan Aplikasi Crypto Map 1

```
1 :   R1(config)#crypto map STTS 10 ipsec-isakmp
2 :   % NOTE: This new crypto map will remain disabled until
      a peer
3 :           and a valid access list have been configured.
4 :   R1(config-crypto-map)# match address 101
5 :   R1(config-crypto-map)# 125.164.4.31
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 fast ethernet 0/1
11 :  R1(config-if)#crypto map STTS
12 :  *Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP
      is ON
```

Dengan demikian konfigurasi dari Router 1 yang terletak pada jaringan Laboratorium Jaringan Komputer telah selesai. Konfigurasi lengkap Router 1 dapat dilihat pada halaman lampiran.

Meskipun konfigurasi Router 1 sudah selesai dilakukan, akan tetapi pada saat ini tunnel VPN belum terbentuk, sehingga untuk menyempurnakan tunnel VPN, konfigurasi Router 2 pada Jaringan Remote harus diselesaikan terlebih dahulu, sebelum uji coba koneksi dapat dilakukan. Pada saat ini, koneksi antara Router 1 dan Router 2 dipastikan putus, atau tidak ada koneksi yang berkesinambungan. Hal ini terbukti dengan hasil PING dari kedua router yang menyatakan “Destination Host Unreachable”. Hal ini disebabkan karena data yang keluar dari Router 1 mengalami enkapsulasi, sedangkan Router 2 belum memiliki transform set.

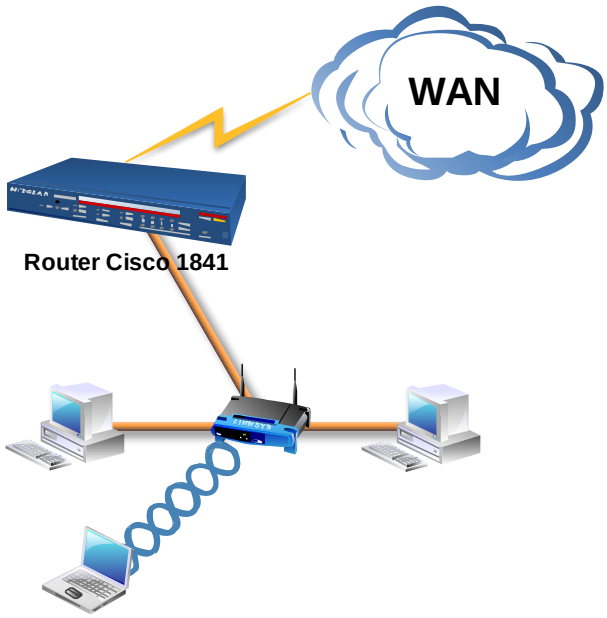
3.2.2. Jaringan Remote

Jaringan Remote merupakan sebuah jaringan independen di luar STTS yang mempunyai koneksi Internet melalui sebuah jalur ADSL. Jaringan ini

terhubung dengan sebuah wireless router untuk membagi koneksi antara beberapa perangkat baik melalui kabel maupun nirkabel.

Router Cisco 1841 dimodifikasi dengan penambahan sebuah modul WIC-1ADSL, dengan sebuah interface RJ-11 yang merupakan pasangan dari konektor kabel telepon. Sehingga fungsi Router Cisco 1841 dapat langsung menggantikan fungsi Router ADSL.

Pada jaringan ini, interface Fast Ethernet 0/0 dari Router Cisco 1841 memiliki alamat IP 202.154.18.1/24 yang, terhubung dengan sebuah Wireless Router dengan alamat IP 202.154.18.2/24. Komputer client terhubung dengan Wireless router ini, baik melalui kabel, maupun nirkabel dengan jaringan 192.168.14.0/24. Ilustrasi Jaringan Remote dapat dilihat pada gambar di bawah ini.



Gambar 3.9
Jaringan Remote

Berikut ini tahap-tahap konfigurasi yang dilakukan pada Router 2 yang berada pada Jaringan Remote.

1. Konfigurasi alamat IP Fast Ethernet 0/0

   Interface ini berfungsi sebagai interface yang terhubung pada jaringan lokal pada Router 2.

Listing 3.18 Konfigurasi Alamat IP Fa0/0 Router 2

```
1 :   R2# configure terminal
2 :   Enter configuration commands, one per line.  End with
      CNTL/Z.
3 :   R2(config)# interface fast ethernet 0/0
4 :   R2(config-if)# ip address 202.154.18.1 255.255.255.0
5 :   R2(config-if)# no shutdown
6 :   R2(config-if)# end
```

2. Konfigurasi Interface ADSL

   Modul Interface ADSL yang dimiliki oleh router harus diatur sedemikian rupa, sehingga router Cisco 1841 memiliki fungsi seperti layaknya router ADSL biasa.

   Listing 3.19 Konfigurasi Interface ADSL Router 2

```
1 :   R2# configure terminal
2 :   R2(config)# interface atm 0
3 :   R2(config-if)# pvc 0/35
4 :   R2(config-if-atm-vc)# encapsulation aal5mux ppp dialer
5 :   R2(config-if-atm-vc)# dialer pool-member 1
6 :   R2(config-if-atm-vc)# no shut
7 :   R2(config-if-atm-vc)# end
```

3. Konfigurasi Dialer

   Pengaturan dialer Router 2 tidak jauh berbeda dengan dialer Router 1, di mana dialer Router 1 bekerja pada interface Fast Ethernet, sedangkan pada Router 2, dialer bekerja pada interface ADSL.

   Listing 3.20 Konfigurasi Dialer Router 2

```
1 :   R2# configure terminal
2 :   R2(config)# interface dialer 1
3 :   R2(config-if)# ip address negotiated
4 :   R2(config-if)# ip mtu 1452
5 :   R2(config-if)# no ip directed-broadcast
6 :   R2(config-if)# ip nat outside
7 :   R2(config-if)# encapsulation ppp
8 :   R2(config-if)# dialer pool 1
9 :   R2(config-if)# ppp authentication pap callin
10 :  R2(config-if)# ppp chap hostname
      152404209***@telkom.net
11 :  R2(config-if)# ppp chap password A***I***F
12 :  R2(config-if)# ppp pap sent-username
      152404209***@telkom.net password A***I***F
13 :  R2(config-if)# end
```

4. Konfigurasi Default Route Dialer 1

   Default route berfungsi untuk menjadikan interface dialer sebagai interface untuk menuju jaringan publik.

   Listing 3.21 Konfigurasi Default Route Dialer 1 Router 2

```
1 :   R2# configure terminal
2 :   R2(config)# ip route 0.0.0.0 0.0.0.0 dialer1
3 :   R2(config)# end
```

5. Konfigurasi Network Address Translation

   Konfigurasi NAT ini berfungsi sebagai penerjemah alamat IP penerima ketika paket yang dikirimkan keluar jaringan kembali diterima oleh router.

   Listing 3.22 Konfigurasi NAT Router 2

```
1 :   R2# configure terminal
2 :   R2(config)#ip nat inside source list 1 interface
      dialer1 overload
3 :   R2(config)#access-list 1 permit 202.154.18.0 0.0.0.255
4 :   R2(config)#end
```

6. Pembentukan IKE Policies dan Pre-shared Key

   Parameter IKE policies pada Router 2 diatur sama dengan parameter IKE policies pada Router 1. Begitu pula dengan Pre-shared Key.

   Listing 3.23 Konfigurasi IKE dan Pre-shared Key Router 2

```
1 :   R2# configure terminal
2 :   R2(config)# crypto isakmp enable
3 :   R2(config)# crypto isakmp policy 10
4 :   R2(config-isakmp)# authentication pre-share
5 :   R2(config-isakmp)# encryption aes 192
6 :   R2(config-isakmp)# hash md5
7 :   R2(config-isakmp)# group 5
8 :   R2(config-isakmp)# lifetime 3600
9 :   R2(config)# crypto isakmp key cisco address
      110.139.62.48
```

7. Konfigurasi IPSec Transform Set

   Sama dengan IKE policies, IPSec Transform Set diatur dengan parameter yang serupa dengan Router 1.

   Listing 3.24 Konfigurasi IPSec Transform Set Router 1

```
1 :   R2(config)# crypto ipsec transform-set 50 esp-aes 192
      esp-md5-hmac
2 :   R2(cfg-crypto-trans)# exit
```

8. Pendefinisian jalur khusus pada Access List

   Tujuan utama pendefinisian ini adalah untuk memberikan akses paket dari kedua ujung gateway untuk melewati firewall pada router, di mana jalur di antara kedua router tersebut mengalami enkripsi.

   Listing 3.25 Konfigurasi Access List Router 1

```
1 :   R2(config)# access-list permit ip 202.154.17.0
      0.0.0.255 202.154.18.0 0.0.0.255
```

9. Pembuatan dan Aplikasi Crypto Map

   Tugas utama crypto map adalah untuk melakukan verifikasi terhadap parameter-parameter kriptografi dari router gateway VPN di sisi yang lain. Dan memasangkan transform-set pada interface yang bersangkutan.

   Listing 3.26 Pembuatan dan Aplikasi Crypto Map 1

```
1 :   R2(config)#crypto map STTS 10 ipsec-isakmp
2 :   % NOTE: This new crypto map will remain disabled until
      a peer
3 :           and a valid access list have been configured.
4 :   R2(config-crypto-map)#match address 101
5 :   R2(config-crypto-map)# set peer 110.139.62.48
6 :   R2(config-crypto-map)# set pfs group5
7 :   R2(config-crypto-map)# set transform-set 50
8 :   R2(config-crypto-map)# set security-association
      lifetime seconds 900
9 :   R2(config-crypto-map)# exit
10 :  R2(config)# interface atm 0/0/0
11 :  R2(config-if)#crypto map STTS
12 :  *Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP
      is ON
```

Dengan demikian konfigurasi dari Router 2 yang terletak pada Jaringan Remote telah selesai. Sehingga uji coba koneksi antara kedua router yang bertindak sebagai gateway VPN dapat dilakukan. Uji coba dilakukan dengan melakukan PING dari router.

Listing 3.27 PING Test

```
1 :   R1#ping
2 :   Protocol [ip]:
3 :   Target IP address: 202.154.18.1
4 :   Repeat count [5]:
5 :   Datagram size [100]:
6 :   Timeout in seconds [2]:
7 :   Extended commands [n]: y
8 :   Source address or interface: 202.154.17.1
9 :   Type of service [0]:
10 :  Set DF bit in IP header? [no]:
```

Listing 3.27 PING Test (Lanjutan)

```
11 :  Validate reply data? [no]:
12 :  Data pattern [0xABCD]:
13 :  Loose, Strict, Record, Timestamp, Verbose[none]:
14 :  Sweep range of sizes [n]:
15 :  Type escape sequence to abort.
16 :  Sending 5, 100-byte ICMP Echos to 202.154.18.1, timeout is 2
      seconds:
17 :  Packet sent with a source address of 202.154.17.1
18 :  !!!!!
19 :  Success rate is 100 percent (5/5), round-trip min/avg/max =
      24/31/56 ms
```

Apabila tunnel IPSec sudah terbentuk, proses PING akan mengembalikan hasil reply dari perangkat remote. Selain itu, tunnel IPSec juga dapat dilihat melalui statistik dari router. Berikut ini potongan dari identifikasi IPsec SA, identifikasi SA selengkapnya dapat dilihat pada halaman lampiran.

Listing 3.28 Identifikasi IPsec SA

```
1 :   R1#show crypto ipsec sa
2 :   interface: Dialer1
3 :       Crypto map tag: SDM_CMAP_1, local addr 110.139.62.48
4 :
5 :      protected vrf: (none)
6 :      local  ident (addr/mask/prot/port):
      (202.154.17.0/255.255.255.0/0/0)
7 :      remote ident (addr/mask/prot/port):
      (202.154.18.0/255.255.255.0/0/0)
8 :      current_peer 125.164.4.31 port 500
9 :        PERMIT, flags={origin_is_acl,}
10 :      #pkts encaps: 34, #pkts encrypt: 34, #pkts digest: 34
11 :      #pkts decaps: 34, #pkts decrypt: 34, #pkts verify: 34
12 :      #pkts compressed: 0, #pkts decompressed: 0
13 :      #pkts not compressed: 0, #pkts compr. failed: 0
14 :      #pkts not decompressed: 0, #pkts decompress failed: 0
15 :      #send errors 1, #recv errors 0
16 :       local crypto endpt.: 110.139.62.48, remote crypto
      endpt.: 125.164.4.31
```

Dengan demikian, tunnel IPsec telah terbentuk dan komunikasi antara kedua jaringan yang bersangkutan dapat berlangsung dengan aman.