
**TUGAS
KEAMANAN SISTEM LANJUT
(EC7010)**

PROTOKOL L2TP

**OLEH
NOVIE THERESIA BR. PASARIBU
(23202107)**



**MAGISTER TEKNOLOGI INFORMASI – TEKNIK ELEKTRO
INSTITUT TEKNOLOGI BANDUNG
2004**

DAFTAR ISI

DAFTAR ISI

DAFTAR GAMBAR

I. PENDAHULUAN

II. VIRTUAL PRIVATE NETWORK (VPN)

III. PROTOKOL L2TP

III.1. PROTOKOL VIRTUAL PPP

III.2. PERANGKAT L2TP

III.3. TUNNEL L2TP

III.3.1. Model Compulsory L2TP

III.3.2. Model Voluntary L2TP

III.4. STRUKTUR PROTOKOL L2TP

III.5. FORMAT HEADER L2TP

III.6. TIPE CONTROL MESSAGE

III.7. AVP (ATTRIBUTE VALUE PAIR)

III.8. CARA KERJA L2TP

III.9. PEMBENTUKAN KONEKSI KONTROL

III.10. AUTENTIFIKASI TUNNEL PADA L2TP

III.11. INCOMING CALL PADA L2TP

III.12. PENGIRIMAN FRAME PPP

III.13. PEMUTUSAN SESSION

III.14. L2TP OVER UDP/IP

III.15. KEAMANAN INFORMASI PADA L2TP

IV. KESIMPULAN

DAFTAR PUSTAKA

DAFTAR GAMBAR

Gambar 1. VPN

Gambar 2. Perkembangan Peluang dan Layanan VPN di Dunia

Gambar 3. Remote Client berbasis PPP menggunakan Dial-in

Gambar 4. Susunan Protokol PPP

Gambar 5. Perangkat L2TP

Gambar 6. Model Compulsory L2TP

Gambar 7. Model Voluntary L2TP

Gambar 8. Struktur Protokol L2TP

Gambar 9. Format Header L2TP

Gambar 10. Format AVP

Gambar 11. Cara Kerja L2TP

Gambar 12. Pembentukan Koneksi Kontrol

Gambar 13. Incoming Call pada L2TP

Gambar 14. Pemutusan Session

I. PENDAHULUAN

Kebutuhan akan perluasan jaringan data/multimedia pada perusahaan sekarang ini semakin tinggi. Perluasan dapat berupa pembukaan *host remote system* ataupun *remote client* yang dapat mengakses jaringan korporat, yang menuntut efisiensi dan keamanan pada jaringan yang lebih tinggi. Berbagai solusi ditawarkan untuk membentuk keamanan jaringan yang handal, diantaranya adalah membentuk sebuah jaringan privat dengan *leased line* (saluran sewa) antara jaringan korporat dengan *remote host* atau *remote client*.

Pada saat jaringan privat mempunyai skala jaringan yang kecil atau menengah, investasi yang ditanam tidaklah terlalu menjadi masalah. Tetapi pada saat skala jaringan menjadi besar, hal ini akan menjadi masalah. Karena menyangkut pengembangan investasi yang semakin tinggi, dan ketersediaan akses akan menjadi masalah yang krusial.

Solusi lain yang lebih efisien adalah pembentukan jaringan privat melalui jaringan publik yang sering dikenal dengan VPN (Virtual Private Network). Bentuk jaringan seperti ini membutuhkan sebuah sistem keamanan yang baik sehingga jaringan privat tersebut tidak dapat diakses oleh pengguna yang tidak berwenang. L2TP (Layer 2 Tunneling Protocol) memberikan solusi keamanan yang baik bagi permasalahan diatas dengan cara membentuk *tunnel* (terowongan) pada jaringan publik yang menghubungkan *remote client* dengan jaringan korporat. L2TP menyediakan akses *dial-up* virtual ke jaringan korporat.

II. VIRTUAL PRIVATE NETWORK (VPN)

Jika dibahas dari masing-masing kata dari VPN, yaitu : *Virtual*, *Private* dan *Network*, maka akan diperoleh arti sebagai berikut :

- Maya (*Virtual*)
 - Sumber daya jaringan yang digunakan, merupakan bagian dari sumber daya umum yang digunakan bersama.
 - Bukan suatu hubungan *physical dedicated* pada struktur jaringan.
- Privat (*Private*)
 - Kebebasan dalam *addressing* dan *routing - topological isolation*
 - Keamanan data (*authentication, encryption, integrity*)
- Jaringan (*Network*)
 - Sekumpulan alat-alat jaringan yang saling berkomunikasi satu dengan yang lain melalui beberapa metode *arbitrary* (berubah-ubah).

Sedangkan pengertian dari *Virtual Networking* dan *Private Networking*, yaitu :

- *Virtual Networking*

Menciptakan *tunnel* dalam jaringan yang tidak harus *direct*. Sebuah 'terowongan' diciptakan melalui jaringan publik seperti Internet. Jadi seolah-olah ada hubungan *point-to-point* dengan data yang dienkapsulasi. ^[6]
- *Private Networking*

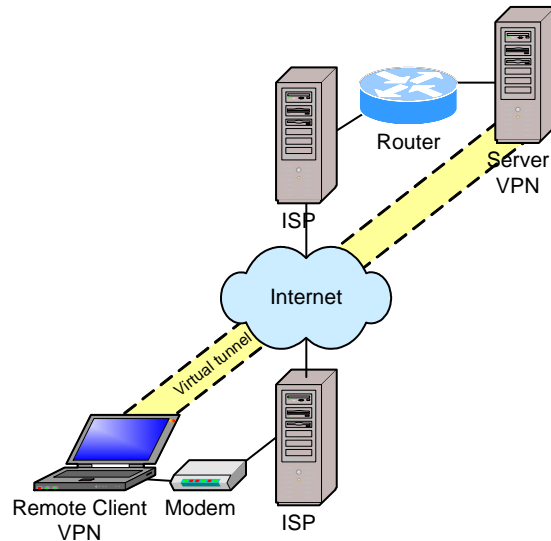
Data yang dikirimkan terenkripsi, sehingga tetap rahasia meskipun melalui jaringan publik. ^[6]

Dari beberapa sumber yang diperoleh, VPN memiliki arti menyeluruh yaitu :

- Suatu jaringan privat yang dibangun dalam infrastruktur jaringan publik, seperti internet yang global.^[11,16]
- Sekumpulan jaringan yang dibangun pada suatu infrastruktur jaringan yang digunakan secara bersama.^[18]
- Suatu VPN menghubungkan komponen-komponen dari satu jaringan diatas jaringan bersama yang lain dengan melindungi transmisi/ proses pengirimannya.^[18]
- Suatu jaringan data privat yang menggunakan infrastruktur telekomunikasi publik, diberikan kebebasan dalam menggunakan suatu protokol *tunneling* dan prosedur keamanan.^[17]
- Suatu jaringan privat yang menggunakan teknologi jaringan publik yang akan datang seperti Internet, pembawa/pengangkut IP, Frame Relay, dan ATM sebagai *backbone wide area network (WAN)*.^[16]

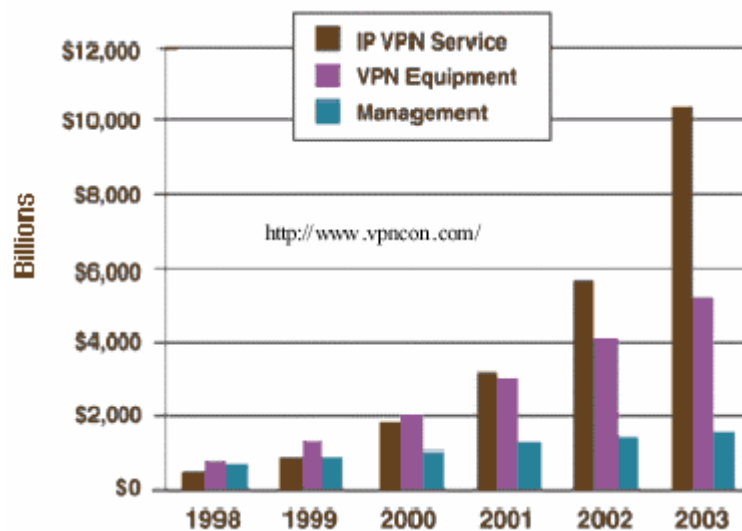
- Suatu perluasan jaringan privat bisnis yang aman melalui suatu jaringan publik.^[15]

Dapat disimpulkan bahwa *Virtual Private Network* adalah suatu jaringan privat yang dibangun pada suatu infrastruktur jaringan publik (misalnya : internet), yang keamanan datanya terjamin.



Gambar 1. VPN

Tingginya persaingan bisnis sekarang ini, menyebabkan banyak perusahaan mulai melirik ke teknologi VPN. Hal ini dapat dilihat dari studi terhadap peluang potensi pasar terhadap VPN dari tahun 1998 hingga tahun 2003 (sumber telechoice.com)^[14]. Dari tabel dibawah ini dapat dilihat terjadi peningkatan yang signifikan dari tahun ke tahun, terutama di tahun 2003.



Gambar 2. Perkembangan Peluang dan Layanan VPN di Dunia

Faktor-faktor yang memicu perusahaan-perusahaan beralih ke VPN, adalah sebagai berikut :

- Ekonomi
 - Dapat mengurangi kebutuhan yang cukup mahal akan saluran sewa (*leased line*) dan panggilan jarak jauh/ biaya interlokal.
 - Efisiensi terhadap kebutuhan saluran telepon perusahaan.
 - Mengurangi biaya operasional.
 - Karena menggunakan infrastruktur publik maka biaya jaringan lebih murah, dapat menghemat 20-47% biaya WAN dan 60-80% untuk biaya *dial-up* akses *remote* (Penelitian dari Infonetics).
- Keleluasaan dalam berkomunikasi/ mudah
 - Jaringan perusahaan dan sumber dayanya bisa di akses kapanpun dan dimana saja diinginkan, karena akses internet yang sudah tersedia diseluruh dunia.
 - Peningkatan fleksibilitas dan pengopersian yang mudah.
- Akses Kontrol
 - Akses ke jaringan perusahaan bisa dilakukan oleh pengguna yang *mobile*, *partner bisnis*, *customer* dan *supplier*.
- Keamanan
 - Jika dibutuhkan, data yang dilewatkan dapat diacak (*encrypted*).
 - Menjamin pihak ketiga yang tidak berwenang tidak dapat menggunakan jaringan virtual.
- Penempatan peralatan yang virtual
 - Dengan adanya ISP, tidak mengurus pembangunan dan pengurusan terhadap *pool modem*.
 - *Host* pada jaringan tidak memerlukan *co-located*.

Untuk menjamin koneksi yang aman antara kedua segmen, yaitu : server perusahaan dan *remote klien*/ ISP melalui jaringan publik (internet), maka teknologi *tunneling* dan *encryption* dilakukan pada VPN.

Dengan *tunneling*, antara kedua segmen VPN dapat berkomunikasi satu dengan yang lain menggunakan protokol tunneling yang sama, dan sebuah *tunnel* dibuat khusus sehingga paket data dapat dikirim melalui internet. Penerapan enkripsi pada VPN, membuat data-data rahasia perusahaan tidak terlihat transparan oleh *sniffer*.

Teknologi *tunneling* dikelompokkan secara garis besar berdasarkan protokol *tunneling layer* 2 (Data Link Layer) dan *layer* 3 (Network Layer) model OSI layer :

- *Tunneling Layer* 2 (Data Link Layer) :
 - L2F (Layer 2 Forwarding)
 - PPTP (Point to Point Tunneling Protocol)
 - L2TP (Layer 2 Tunneling Protocol)

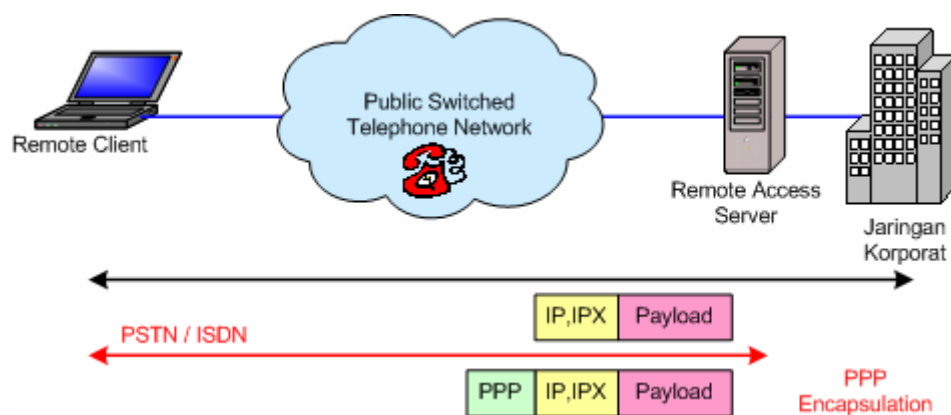
-
- *Tunnelling Layer 3* (Network Layer):
 - IPSec (IP Security)
 - VTP (Virtual Tunneling Protocol)
 - ATMP (Ascend Tunnel Management Protocol)

L2TP adalah suatu standard IETF (RFC 2661) pada *layer 2* yang merupakan kombinasi dari keunggulan-keunggulan fitur dari protokol L2F (dikembangkan oleh Cisco) dan PPTP (dikembangkan oleh Microsoft), yang didukung oleh vendor-vendor : Ascend, Cisco, IBM, Microsoft dan 3Com. Untuk mendapatkan tingkat keamanan yang lebih baik , L2TP dapat dikombinasikan dengan protocol *tunneling* IPSec pada *layer 3*.

III. PROTOKOL L2TP

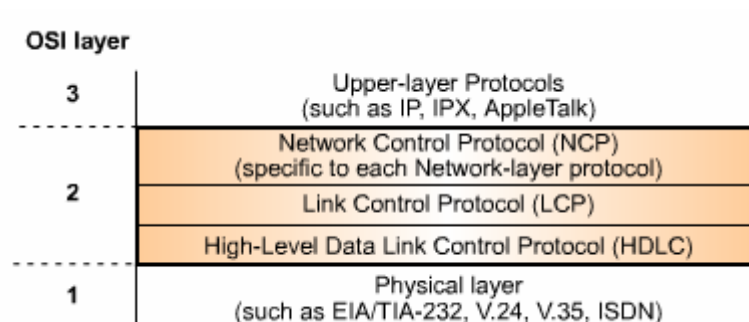
Protokol L2TP sering juga disebut sebagai protokol *dial-up* virtual, karena L2TP memperluas suatu *session* PPP (Point-to-Point Protocol) *dial-up* melalui jaringan publik internet, atau sering juga digambarkan seperti koneksi virtual PPP.

III.1. PROTOKOL VIRTUAL PPP



Gambar 3. Remote Client berbasis PPP menggunakan Dial-in

PPP menggambarkan suatu mekanisme enkapsulasi untuk mengangkut paket-paket multiprotocol melalui hubungan *point-to-point* pada layer 2.



Gambar 4. Susunan Protokol PPP

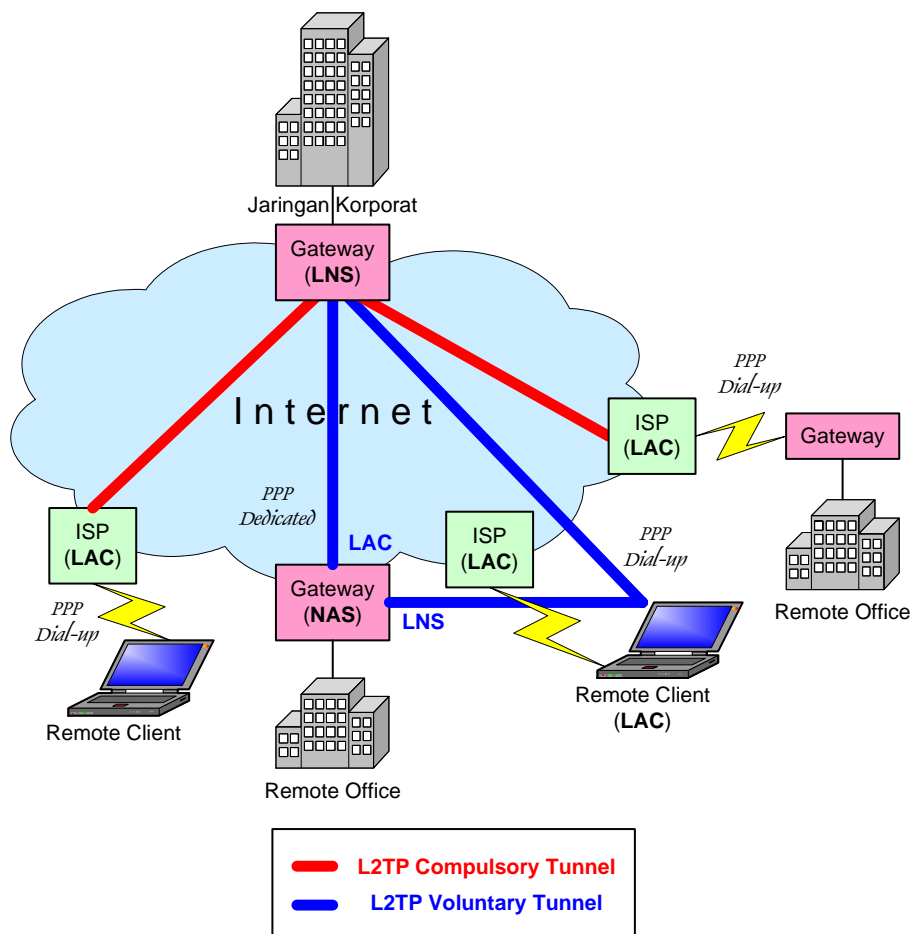
PPP terdiri dari 4 komponen utama yaitu :

1. EIA/TIA 232 : Layer fisik untuk komunikasi serial.
2. HDLC : Metode untuk enkapsulasi datagram melalui link serial.
3. LCP : Metode untuk pembentukan, konfigurasi, mempertahankan, dan memutuskan jaringan PPP.
4. NCP : Metode pembentukan dan mengkonfigurasi protokol *Network Layer* yang berbeda (Layer 3 : misalnya IP, IPX, atau apple talk).

Terdapat 2 metode autentifikasi pada PPP :

1. PAP (Password Authentication Protocol)
2. CHAP (Challenge Authenticoitin Protocol)

III.2. PERANGKAT L2TP



Gambar 5. Perangkat L2TP

Perangkat dasar L2TP :

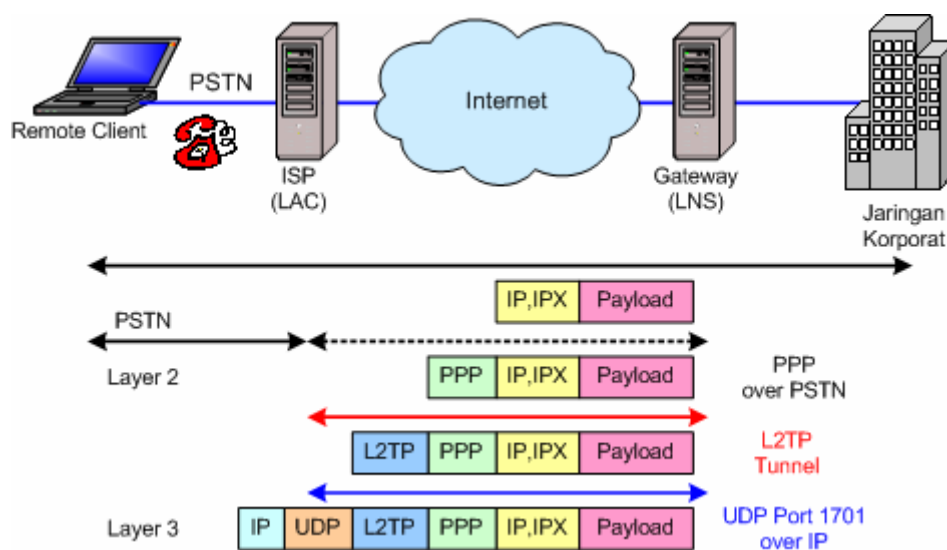
- *Remote Client*
 - Suatu *end system* atau *router* pada jaringan *remote access* (mis. : *dial-up client*).
- L2TP Access Concentrator (LAC)
 - Sistem yang berada disalah satu ujung *tunnel* L2TP dan merupakan *peer* ke LNS.
 - Berada pada sisi *remote client/ ISP*.
 - Sebagai pemrakarsa *incoming call* dan penerima *outgoing call*.
- L2TP Network Server (LNS)
 - Sistem yang berada disalah satu ujung *tunnel* L2TP dan merupakan *peer* ke LAC.
 - Berada pada sisi jaringan korporat.
 - Sebagai pemrakarsa *outgoing call* dan penerima *incoming call*.
- Network Access Server (NAS)
 - NAS dapat berlaku seperti LAC atau LNS atau kedua-duanya.

III.3. TUNNEL L2TP

Skenario L2TP adalah untuk membentuk *tunnel* atau terowongan frame PPP antara *remote client* dengan LNS yang berada pada suatu jaringan korporat.

Terdapat 2 model tunnel L2TP yang dikenal , yaitu *compulsory* dan *voluntary*. Perbedaan utama keduanya terletak pada *endpoint tunnel*-nya. Pada *compulsory tunnel*, ujung *tunnel* berada pada ISP, sedangkan pada *voluntary* ujung *tunnel* berada pada *client remote*.

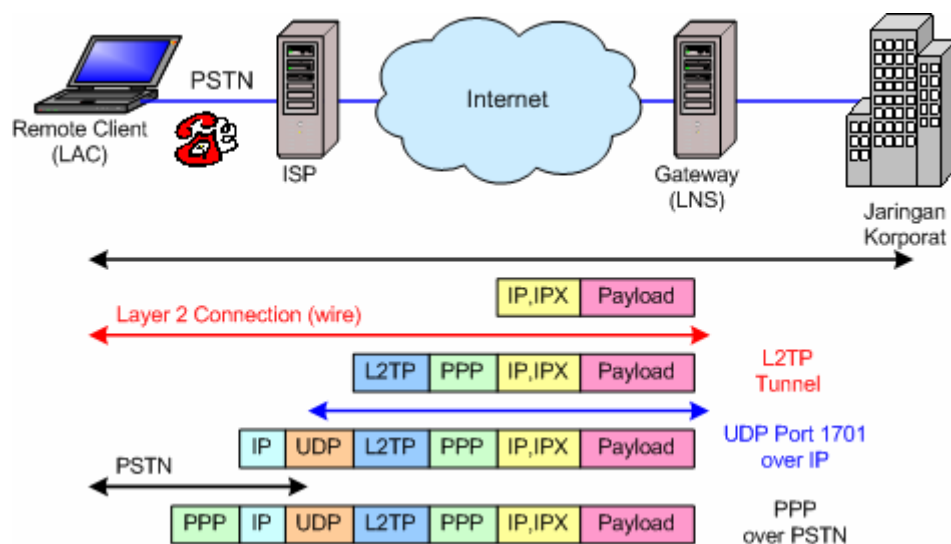
III.3.1. Model Compulsory L2TP



Gambar 6. Model Compulsory L2TP

1. *Remote client* memulai koneksi PPP ke LAC melalui PSTN. Pada gambar diatas LAC berada di ISP.
2. ISP menerima koneksi tersebut dan *link* PPP ditetapkan.
3. ISP melakukan *partial authentication* (pengesahan parsial) untuk mempelajari *user name*. *Database map user* untuk layanan-layanan dan *endpoint tunnel* LNS, dipelihara oleh ISP.
4. LAC kemudian menginisiasi *tunnel* L2TP ke LNS.
5. Jika LNS menerima koneksi, LAC kemudian mengencapsulasi PPP dengan L2TP, dan meneruskannya melalui *tunnel* yang tepat.
6. LNS menerima *frame-frame* tersebut, kemudian melepaskan L2TP, dan memprosesnya sebagai *frame incoming* PPP biasa.
7. LNS kemudian menggunakan pengesahan PPP untuk memvalidasi *user* dan kemudian menetapkan alamat IP.

III.3.2. Model Voluntary L2TP



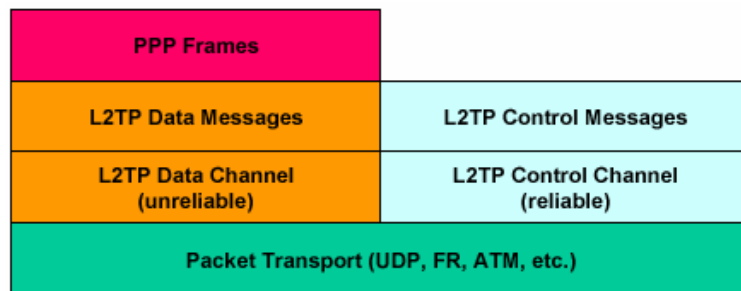
Gambar 7. Model Voluntary L2TP

1. *Remote client* mempunyai koneksi *pre-established* ke ISP. Remote Client berfungsi juga sebagai LAC. Dalam hal ini, *host* berisi *software client* LAC mempunyai suatu koneksi ke jaringan publik (internet) melalui ISP.
2. *Client* L2TP (LAC) menginisiasi *tunnel* L2TP ke LNS.

3. Jika LNS menerima koneksi, LAC kemudian meng-encapsulasi PPP dengan L2TP, dan meneruskannya melalui *tunnel*.
4. LNS menerima *frame-frame* tersebut, kemudian melepaskan L2TP, dan memprosesnya sebagai *frame incoming* PPP biasa.
5. LNS kemudian menggunakan pengesahan PPP untuk memvalidasi *user* dan kemudian menetapkan alamat IP.

III.4. STRUKTUR PROTOKOL L2TP

Ada dua jenis *messages* yang digunakan L2TP : *control messages* dan *data messages*.



Gambar 8. Struktur Protokol L2TP

Control messages	Data messages
Digunakan untuk : <ul style="list-style-type: none"> ▫ <i>Establishment</i> (pembentukan) ▫ <i>Maintenance</i> (pemeliharaan) ▫ Pemutusan <i>tunnel</i> L2TP dan interkoneksi 	Digunakan untuk : <ul style="list-style-type: none"> ▫ Mengenkapsulasi <i>frame</i> PPP yang akan dibawa melalui <i>tunnel</i>
Menggunakan suatu <i>control channel</i> yang <i>reliable</i> didalam L2TP untuk menjamin kepastian paket yang terkirim.	Jika <i>loss packet</i> terjadi, <i>data message</i> tidak akan di kirim kembali (<i>not reliable</i>).

Keterangan gambar :

Frame PPP dienkapsulasi oleh *header* L2TP dan paket *transport* (UDP, *Frame Relay*, ATM, dll), kemudian dilewatkan melalui *data channel* yang *unreliable*. *Control messages* dikirimkan melalui suatu *control channel* L2TP yang juga mentransmisikan paket *in-band* melalui paket *transport* yang sama.

-
- Ver : - Ver = 2, versi header *data message* L2TP
 - Jika *unknown Ver*, paket tersebut harus dibuang.
- Length field : - Panjang total dari *message* (byte).
- Tunnel ID : - *Identifier* untuk *control connection*
 - *Significant* lokal saja
- Session ID : - *Identifier* untuk suatu *session* di dalam suatu *tunnel*.
 - *Significant* lokal saja
- Ns Sequence Number : - *Sequence number* untuk *control message*
- Nr Sequence Number : - *Sequence number control message* berikutnya yang diterima.
- Offset Field : - *Start* dari *payload data*

III.6. TIPE CONTROL MESSAGE

Di dalam protokol *tunnel*, *control message* dipertukarkan secara *in-band* antara LAC dan LNS. Kontrol koneksi bertanggung jawab untuk pembentukan, pemutusan, dan *maintenance session*, yang dibawa didalam *tunnel* dan *tunnel* itu sendiri.

Tipe *control message* adalah sebagai berikut :

Control Connection Management

0	(reserved)	
1	(SCCRQ)	Start-Control-Connection-Request
2	(SCCRP)	Start-Control-Connection-Reply
3	(SCCCN)	Start-Control-Connection-Connected
4	(StopCCN)	Stop-Control-Connection-Notification
5	(reserved)	
6	(HELLO)	Hello

Call Management

7	(OCRO)	Outgoing-Call-Request
8	(OCRP)	Outgoing-Call-Reply
9	(OCCN)	Outgoing-Call-Connected
10	(ICRQ)	Incoming-Call-Request
11	(ICRP)	Incoming-Call-Reply
12	(ICCN)	Incoming-Call-Connected
13	(reserved)	
14	(CDN)	Call-Disconnect-Notify

Error Reporting

15	(WEN)	WAN-Error-Notify
----	-------	------------------

PPP Session Control

16	(SLI)	Set-Link-Info
----	-------	---------------

Definisi *control message* diatas adalah sebagai berikut :

- **SCCRQ** - *control message* yang digunakan untuk menginisialisasi *tunnel* antara LNS dan LAC. Dikirim oleh LAC dan LNS untuk proses pembentukan *tunnel*.
- **SCCRP** - *control message* digunakan untuk mengindikasikan bahwa SCCRW telah diterima dan pembentukan *tunnel* harus dilanjutkan. Dikirim sebagai balasan dari *message* SCCRQ yang dikirim.
- **SCCN** - *control message* yang menyelesaikan proses pembentukan *tunnel*. Dikirim sebagai jawaban dari SCCRP.
- **StopCCN** - *control message* yang dikirim oleh LAC dan LNS untuk menginformasikan *peer* bahwa *tunnel* sedang di putus dan hubungan kontrol harus diputus. Lebih lanjut lagi seluruh seluruh koneksi akan terputus (tanpa mengirim *explicit call control message*).
- **OCRQ** - *control message* yang dikirim oleh LNS ke LAC untuk mengindikasikan bahwa *outbond call* dari LAC terbentuk. Merupakan *message* pertama dalam pertukaran *message* yang digunakan untuk membentuk *session* dalam *tunnel* L2TP.
- **OCRP** - *control message* yang dikirim oleh LAC kepada LNS sebagai respon OCRQ yang dikirim. Merupakan *message* kedua yang betukar pada pembentukan *session* dalam *tunnel* L2TP.
- **OCCN** - *control message* yang dikirimkan LAC ke LNS mengikuti OCRP setelah *outgoing call* terbentuk. Merupakan *message* terakhir yang bertukar untuk pembentukan *session* dalam *tunnel* L2TP. OCCN digunakan juga untuk mengindikasikan hasil dari permintaan *ougoing call* yang berhasil dan memberikan informasi pada LNS mengenai parameter yang diperoleh setelah panggilan terbentuk seperti tipe *message*, (TX) *connection speed*, dan tipe *framing*.

III.7. AVP (ATTRIBUTE VALUE PAIR)

Pada L2TP metode pengkodean yang sama/seragam harus digunakan untuk tipe dan *body message*. Pengkodean ini dikenal dengan istilah AVP (Attribute Value Pair).

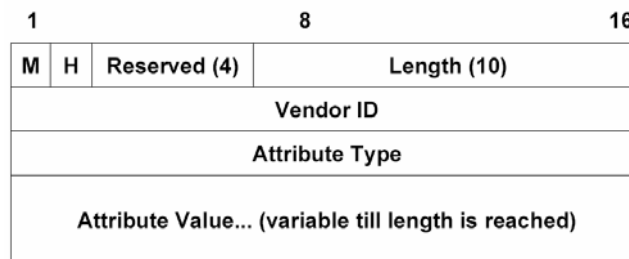
AVP diperlukan untuk pertukaran dan negosiasi informasi *session* L2TP yang lebih detail, seperti : *windows size*, *host name*, *call serial number*, dan sebagainya.

Terdapat beberapa jenis AVP yang biasa digunakan, diantaranya :

- Message Type
- Random Vector
- Result Code
- Protocol Version
- Framing Capabilities
- Bearer Capabilities
- Bearer Type
- Tie Breaker
- Firmware Version
- Host Name
- Vendor Name
- Assigend Tunnel ID

- Receive Windows Size
- Challenge Respons
- Q.931 Cause Code
- Assigned Session ID
- Call Serial Number
- Min dan Max BPS
- Framing Type
- Caller Number
- Calling Number

Format AVP seperti di bawah ini :



Gambar 10. Format AVP

Enam bit pertama adalah *bit mask* yang menunjukkan atribut umum dari AVP. Bit-bit M dan H nilainya didefinisikan, sedangkan bit-bit yang lainnya di *reserve* untuk pengembangan lebih lanjut. Reserve bit = 0.

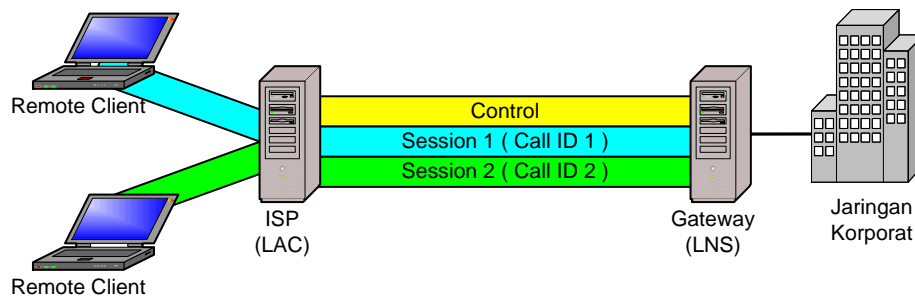
- **Mandatory (M)** - Mengontrol tindakan yang perlu dilakukan jika AVP yang diterima tidak dikenal. Jika bit M diaktifkan pada AVP yang tidak dikenal di dalam *message* pada *session* tertentu, maka *session* yang terkait akan diputuskan.
Jika M bit diaktifkan pada AVP yang tidak dikenal di dalam *message* pada keseluruhan *tunnel*, maka *tunnel* (dan semua *session* didalamnya) akan diputuskan.
Jika M bit tidak diaktifkan, maka AVP yang tidak dikenal akan diabaikan.
- **Hidden (H)** - Mengidentifikasi data yang disembunyikan pada *field Attribute Value* dari sebuah AVP. Digunakan untuk mengatasi data-data sensitif yang dilewatkan misalnya *password user* sebagai *clear text* pada sebuah AVP.
- **Length** - Menunjukkan jumlah octet pada AVP tersebut.
- **Vendor ID** - IANA menentukan nilai "*SMI Network Management Private Enterprise Code*".

III.8. CARA KERJA L2TP

Komponen-komponen pada tunnel, yaitu :

- *Control channel*, fungsinya :
 - *Setup* (membangun) dan *teardown* (merombak) *tunnel*

- *Create* (menciptakan) dan *teardown* (merombak) *payload* (muatan) *calls* dalam *tunnel*.
- Menjaga mekanisme untuk mendeteksi *tunnel* yang *outages*.
- *Sessions* (data channel) untuk *delivery* data :
 - Layanan *delivery payload*
 - Paket *PPP* yang di-encapsulasi dikirim pada *sessions*

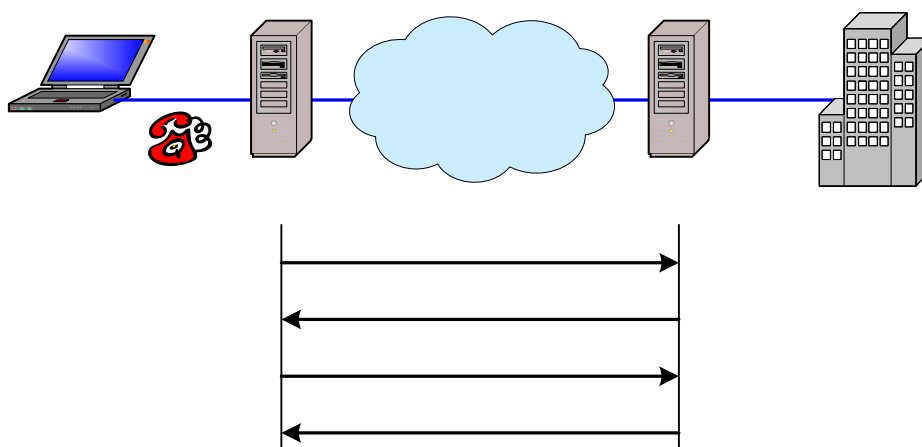


Gambar 11. Cara Kerja L2TP

Ada 2 langkah untuk membentuk *tunnel* untuk *session* PPP pada L2TP :

1. Pembentukan koneksi kontrol untuk suatu *tunnel*.
Sebelum *incoming* atau *outgoing call* dimulai, *tunnel* dan koneksi kontrol harus terbentuk.
2. Pembentukan *session* yang dipicu oleh permintaan *incoming* atau *outgoing call*.
Suatu *session* L2TP harus terbentuk sebelum *frame* PPP dilewatkan pada *tunnel* L2TP. *Multiple session* dapat dibentuk pada satu *tunnel*, dan beberapa *tunnel* dapat dibentuk diantara LAC dan LNS yang sama.

III.9. PEMBENTUKAN KONEKSI KONTROL



Gambar 12. Pembentukan Koneksi Kontrol

Koneksi kontrol adalah koneksi yang paling pertama dibentuk antara LAC dan LNS sebelum *session* terbentuk. Pembentukan koneksi kontrol termasuk menjamin identitas dari *peer*, seperti pengidentifikasi versi L2TP *peer*, *framing*, kemampuan *bearer*, dan sebagainya.

Ada tiga *message* dipertukarkan yang dilakukan untuk membangun koneksi kontrol (SCCRQ, SCCRP, dan SCCN). Jika tidak ada *message* lagi yang menunggu dalam antrian *peer* tersebut, ZLB ACK dikirimkan.

III.10. AUTENTIFIKASI TUNNEL PADA L2TP

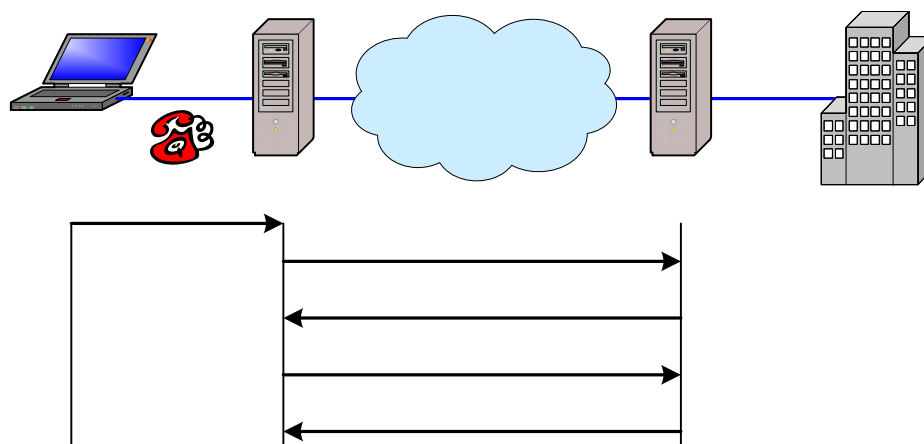
Sistem autentifikasi yang digunakan L2TP, hampir sama dengan CHAP selama pembentukan koneksi kontrol.

Autentifikasi *tunnel* L2TP menggunakan *Challenge* AVP yang termasuk di dalam *message* SCCRQ atau SCCRP :

- Jika *challenge* AVP diterima di SCCRQ atau SCCRP, maka AVP *challenge* respon harus dikirimkan mengikuti SCCRP atau SCCCN secara berturut-turut.
- Jika respon yang diharapkan dan respon yang diterima tidak sesuai, maka pembentukan *tunnel* tidak diijinkan.

Untuk dapat menggunakan *tunnel*, sebuah *password single share* harus ada diantara LAC dan LNS.

III.11. INCOMING CALL PADA L2TP



Gambar 13. Incoming Call pada L2TP

Session individu dapat terbentuk, setelah koneksi kontrol terbentuk dengan berhasil. Setiap *session* berhubungan dengan satu aliran PPP antara LAC dan LNS.

Pembentukan *session* memiliki arah yang sesuai dengan LAC dan LNS. LAC meminta LNS menerima *session* untuk *incoming call*, dan LNS meminta LAC menerima *session* untuk menempatkan *outgoing call*.

Terdapat 3 message yang terlibat dalam pembentukan *session* (ICRQ, ICRP, ICCN). Jika tidak ada *message* lagi yang menunggu dalam antrian *peer* tersebut, ZLB ACK dikirimkan.

III.12. PENGIRIMAN FRAME PPP

Setiap kali *tunnel* terbentuk secara lengkap, maka :

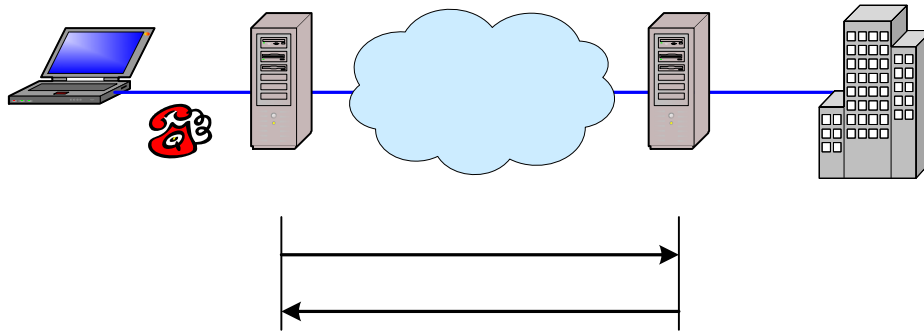
- *Frame* PPP dari *remote client* diterima pada LAC
- *Stripped* (pemotongan) CRC
- Menghubungkan *frame*
- Transparansi byte
- Di-enkapsulasi dalam L2TP
- Diteruskan melalui *tunnel* yang terkait.

LNS menerima paket L2TP dan memproses *frame* PPP yang terenkapsulasi jika paket tersebut diterima di *interface* PPP local. Pengirim *message* dihubungkan dengan *session* dan *tunnel*-nya menempatkan *session* ID dan *tunnel* ID pada *header session* ID dan *tunnel* ID untuk semua *outgoing message*. Dengan cara ini *frame* PPP di multiplex dan demultiplex melalui single *tunnel* antara LAC dan LNS.

Multiple tunnel dapat terbentuk pada sebuah pasangan LAC-LNS, dan *multiple session* dapat terbentuk dalam sebuah *session*.

III.13. PEMUTUSAN SESSION

Dengan cara mengirimkan *control message* CDN, pemutusan *session* dapat dilakukan oleh LAC atau LNS. Setelah *session* terakhir terputus, maka koneksi kontrol dapat diputuskan.



Gambar 14. Pemutusan Session

III.14. L2TP OVER UDP/IP

L2TP menggunakan *port* UDP 1701 yang teregister. Inisiator *tunnel* L2TP akan mengambil satu *port* UDP *source*/asal (yang bukan 1701) dan mengirimkan ke tujuan yang dikehendaki dengan alamat *port* 1701.

Remote Client

Demikian pula penerima akan mengambil sebuah *port* yang bebas (selain 1701) pada sistemnya, dan mengirim balik kepada inisiator dengan alamat *port* UDP (*port* 1701).

Setiap kali *port* asal dan tujuan, dan alamat terbentuk maka alamat *port* yang digunakan pun akan tetap/static. Jika *port* yang digunakan berubah-ubah, maka mekanisme L2TP melewati perangkat NAT akan lebih kompleks.

Fragmentasi IP dapat terjadi pada L2TP seperti paket L2TP melewati melalui substrat IP. L2TP tidak mempunyai perlakuan khusus untuk mengoptimalkannya. Implementasi LAC dapat menyebabkan LCP bernegosiasi nilai MRU, yang mengoptimalkan lingkungan LAC sehingga paket L2TP dapat dilewatkan dengan nilai MTU yang konsisten.

Secara *default* pada beberapa implementasi L2TP UDP *checksum* harus digunakan untuk kontrol dan *data message*. UDP *checksum* pada *data message* boleh tidak digunakan, tetapi penggunaan *checksum* pada *control message* direkomendasikan.

III.15. KEAMANAN INFORMASI PADA L2TP

L2TP membentuk tunnel LAC hingga LNS, sehingga data yang dilewatkan tidak dapat terlihat secara transparan oleh pengguna jaringan publik.

Ada beberapa bentuk keamanan yang diberikan oleh L2TP, yaitu :

- **Keamanan *Tunnel Endpoint***

Prosedur autentifikasi *tunnel endpoint* selama pembentukan tunnel, memiliki atribut yang sama dengan CHAP (Challenge Handshake Authentication Protocol).

Mekanisme ini tidak di desain untuk menyediakan autentifikasi setelah proses pembentukan *tunnel*. Karena bisa saja pihak ketiga yang tidak berhak dapat melakukan pengintaian terhadap aliran data pada *tunnel* L2TP dan melakukan injeksi terhadap paket L2TP, jika setelah proses pembentukan *tunnel* terjadi.

- **Keamanan Level Paket**

Pengamanan L2TP memerlukan keterlibatan *transport* lapisan bawah melakukan layanan enkripsi, integritas, dan autentifikasi untuk semua trafik L2TP. *Transport* yang aman tersebut akan beroperasi pada seluruh paket L2TP dan tidak tergantung fungsi PPP dan protokol yang dibawa oleh PPP.

- **Keamanan *End to End***

Memproteksi aliran paket L2TP melalui *transport* yang aman berarti juga memproteksi data di dalam *tunnel* PPP pada saat diangkut dari LAC menuju LNS. Proteksi seperti ini bukan merupakan pengganti keamanan *end-to-end* antara host atau aplikasi yang berkomunikasi.

- **Kombinasi antara L2TP dan IPsec**

Pada saat berjalan pada IP (layer 3), IPsec dipergunakan untuk mengenkapsulasi paket dan bisa juga dipergunakan untuk enkripsi dalam protokol *tunneling* lainnya. IPsec menyediakan keamanan level paket menggunakan 2 protokol, yaitu :

- AH (Authentication Header)

Memungkinkan verifikasi identitas pengirim dan ada pengecekan integritas dari pesan/ informasi.

- ESP (Encapsulating Security Payload)

Memungkinkan enkripsi informasi sehingga tetap rahasia. IP original dibungkus dan *outer* IP header biasanya berisi *gateway* tujuan. Tidak ada jaminan *integrity* dari *outer* IP *header*, maka digunakan bersama dengan protokol AH.

IPsec menyediakan mode operasi yang dapat melakukan *tunneling* paket IP. Enkripsi dan autentifikasi pada level paket disediakan oleh mode IPsec *tunnel*.

Jadi untuk menjamin keamanan L2TP yang lebih handal digunakan *transport* yang aman dan juga mengimplementasikan IPsec pada *tunneling* layer 3. Metode ini dikenal dengan L2TP *over* IPsec. (lihat tugas : R M Dikshie Fauzie, NIM : 23201093, "Tinjauan Mekanisme dan Aplikasi IPsec : Studi Kasus VPN")

VI. KESIMPULAN

1. Untuk mengembangkan jaringan perusahaan dengan biaya yang relatif rendah dan aman, VPN adalah merupakan salah satu solusinya.
2. Ada beberapa protokol *tunneling* untuk VPN pada layer 2, yaitu : L2F, PPTP dan L2TP.
3. L2TP menghadirkan fitur-fitur yang terbaik yang merupakan kombinasi antara protokol L2F dan PPTP.
4. Ada dua model *tunnel* yang didukung oleh L2TP adalah *compulsory* dan *voluntary*. Perbedaannya pada *end point tunnel*. Pada *compulsory tunnel* berakhir pada ISP dan *voluntary tunnel* berakhir pada *remote client*.
5. L2TP menyediakan metode autentifikasi PPP, yaitu PAP dan CHAP.
6. L2TP menggunakan dua jenis *message*, yaitu *control message* dan *data message*. *Control message* digunakan pada *establishment*, *maintenance* dan *clearing tunnel* dan *call*. *Data message* digunakan untuk meng-enkapsulasi *frame* PPP yang dibawa melalui *tunnel*.
7. Untuk komunikasi *tunnel* L2TP menggunakan *port* UDP 1701.
8. Beberapa jenis keamanan yang disediakan oleh protokol L2TP, yaitu : keamanan *end point tunnel*, keamanan level paket, keamanan *end-to-end*, dan kombinasi antara protokol L2TP dengan IPSec.
9. L2TP (layer 2) dapat dikombinasikan dengan IPSec (layer 3), untuk memberikan koneksi yang lebih aman melalui internet, karena dengan enkapsulasi IPSec menambah kekuatan enkripsi dan autentifikasi.

DAFTAR PUSTAKA

1. Cisco, Fact Sheet : "Layer 2 Tunneling Protocol", <http://www.jimblake.com/>
2. Cisco, Fact Sheet : "Layer 2 Tunneling Protocol, A Key Building Block for an Access Virtual Private Network", <http://www.cisco.com/warp/public/>
3. Cisco, "L2TP Questions and Answers", <http://www.jimblake.com/>
4. Cisco, Technology Brief : "Layer 2 Tunnel Protocol", <http://www.jimblake.com/>
5. Crosstalk, "L2TP Principles", <http://www.crosstalk.at/>
6. Debra Littlejohn Shinder, "Computer Networking Essentials", Cisco Press, Indianapolis, 2001.
7. Gordon Chaffee, "Virtual Private Networks (VPN) Network Address Translation (NAT)", Berkeley Multimedia Research Center University of California, Berkeley, March 19, 1998, <http://bmrc.berkeley.edu/people/chaffee>
8. ITSO Rochester, "Layer 2 Tunneling Protocol (L2TP) Overview", <http://www.ibm.com/>
9. Martin W. Murhammer, "Layer 2 Tunneling Protocol (L2TP)", International Technical Support Center, Raleigh, <http://www.ibm.com/>
10. Martin W. Murhammer, "Virtual Private Networks (VPN)", IBM International Technical Support Organization, Raleigh, NC, <http://www.ibm.com/servers/eserver/series/tcpip/vpn/>
11. Mika Ilvesmäki, "Provider based Virtual Private Networks", Helsinki University of Technology, 4.3.2004, <http://www.netlab.hut.fi/opetus/>
12. Network Working Group, "Layer Two Tunneling Protocol L2TP", Request for Comments: 2661, <http://www.zvon.org/tmRFC/RFC2661/>
13. Prof. Dr. Andreas Steffen, "Virtual Private Networks VPNs", Sichere Netzwerkkommunikation (SNK), <http://www-t.zhwin.ch/it/snk/>
14. Prof. Dr. P. Heinzmann, "Internet Security Course", ITA- HSR and cnlab Information Technology Research AG, <http://www.ita.hsr.ch/nws/>
15. Robert Pitton, "Virtual Private Networks for Wireless LAN Security", 3 com, April 10, 2003, <http://torwug.org/local/>
16. Shang- chieh J. Wu, "The Introduction of Virtual Private Network", Oct 25 2002, <http://www.cs.umd.edu/>
17. VPN Consortium, "VPN Technologies: Definitions and Requirements", January 2003, <http://www.vpnc.org/>
18. 虛擬私有網路, TWNIC 2003, <http://map.twnic.net.tw/iptraining/doc/>