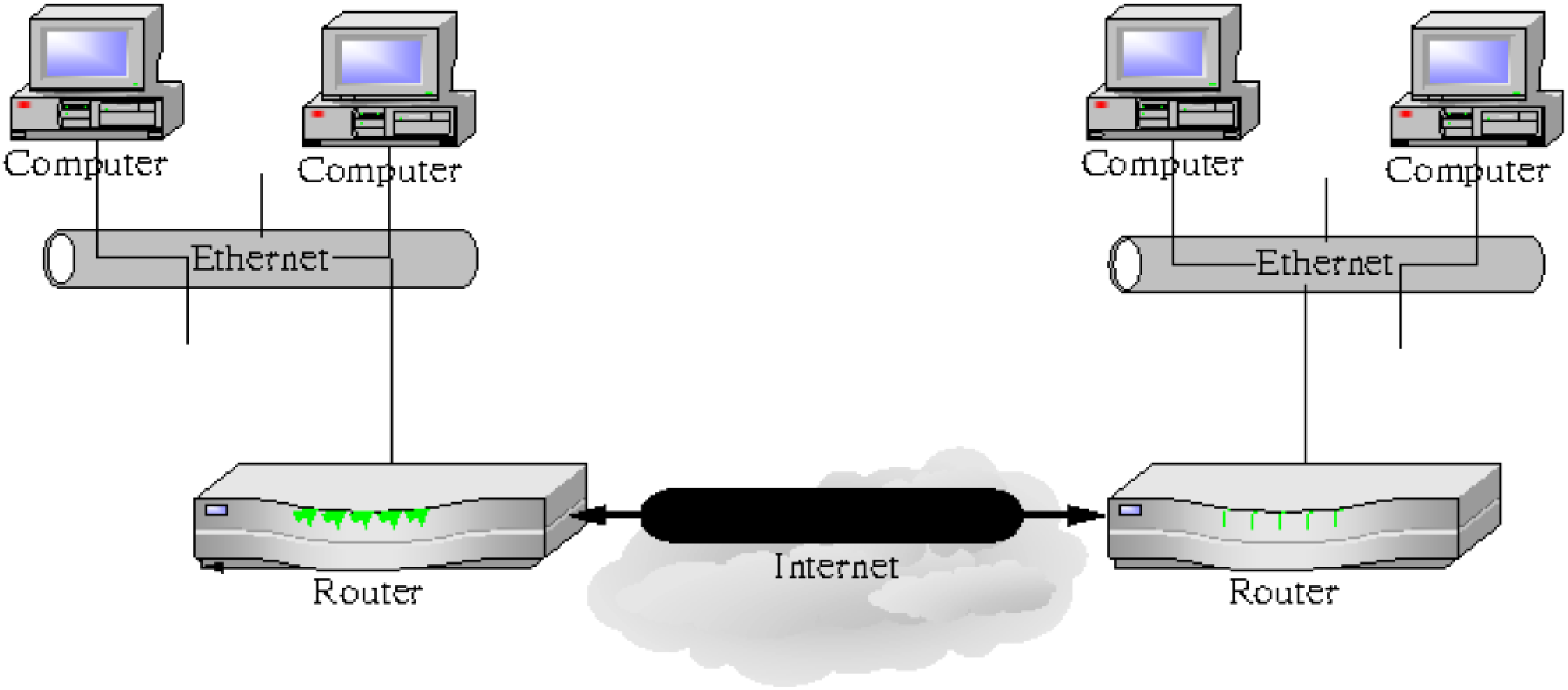
Virtual Private Network

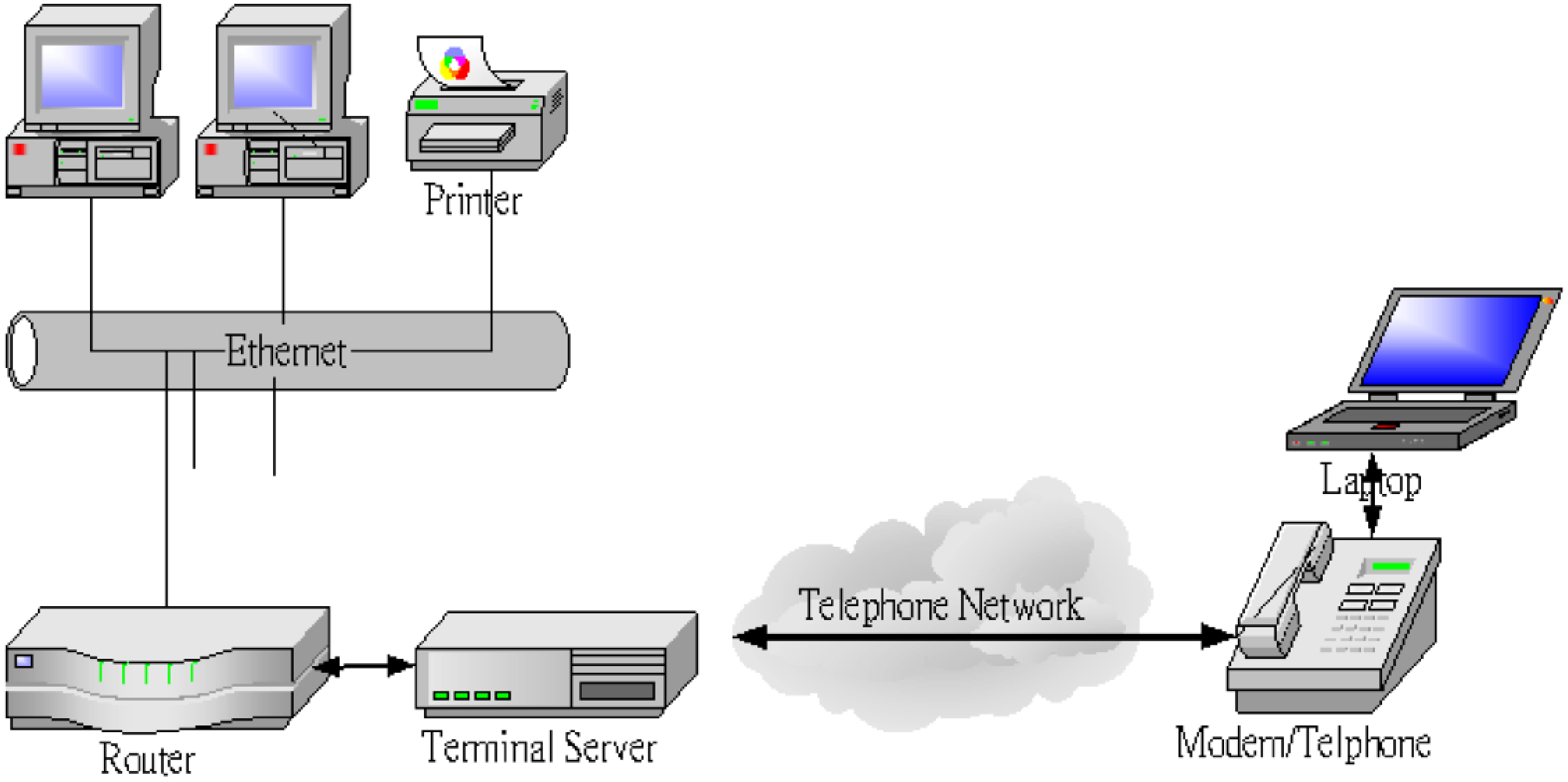
What is a VPN

- ❑ Used to connect two private networks together via the Internet



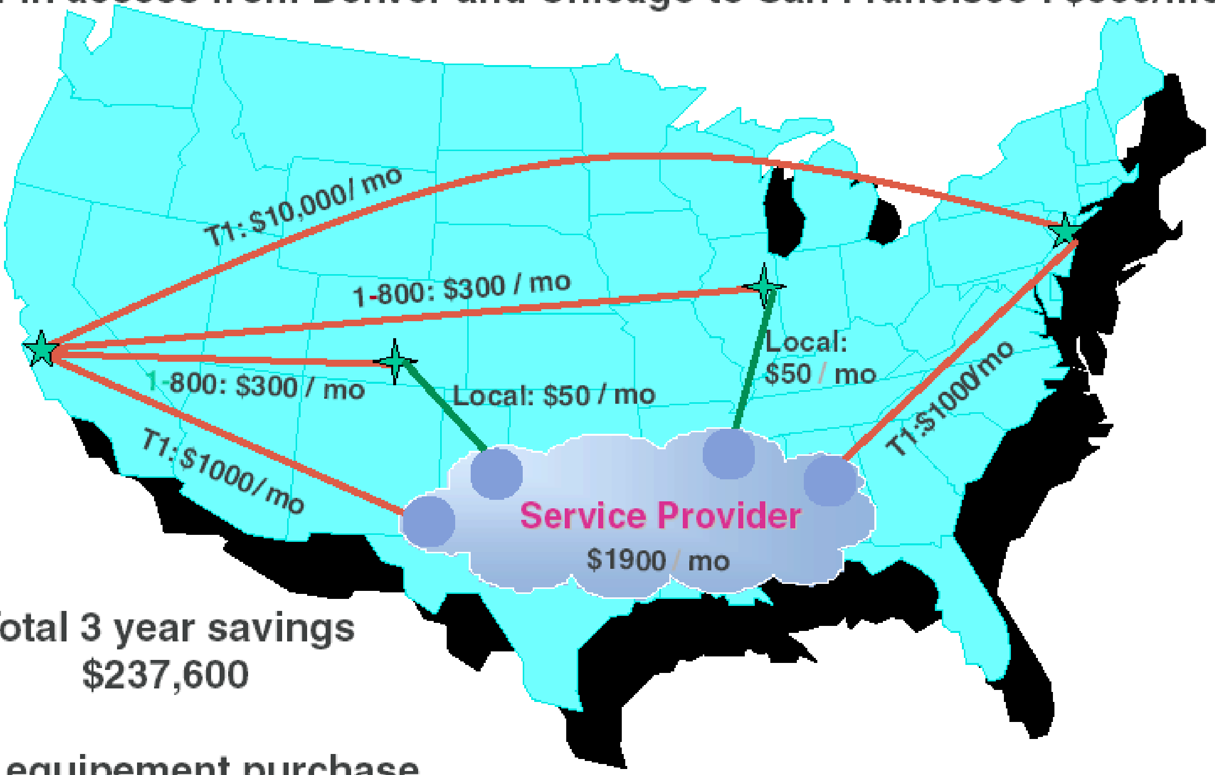
What is a VPN

- Used to connect remote users to a private network via the Internet



Why ?

T1 connections between San Francisco and New York City : $10,000/mo
Dial-in access from Denver and Chicago to San Francisco : $600/mo

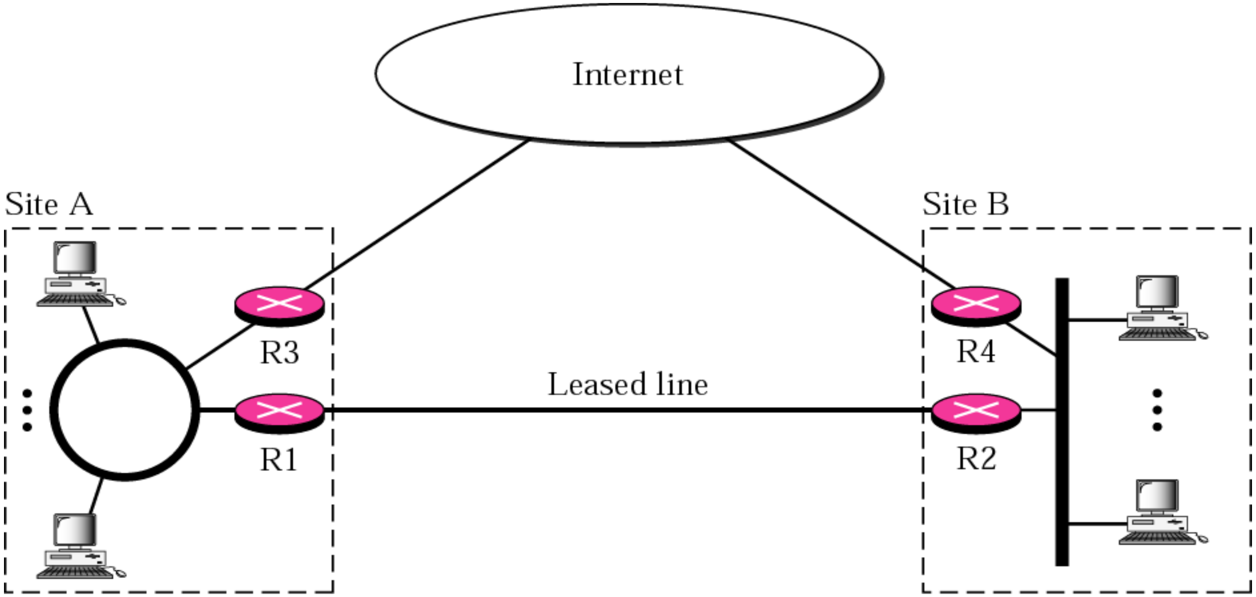


Total 3 year savings
$237,600

VPN equipement purchase
$7,800

Virtual Private Network

- ❑ VPN connects the components of one network over another network by tunnel through the public network with security and features formerly available only in private network
- ❑ VPN saves the cost of dedicated line
- ❑ Brief: VPN is Secure Tunnel

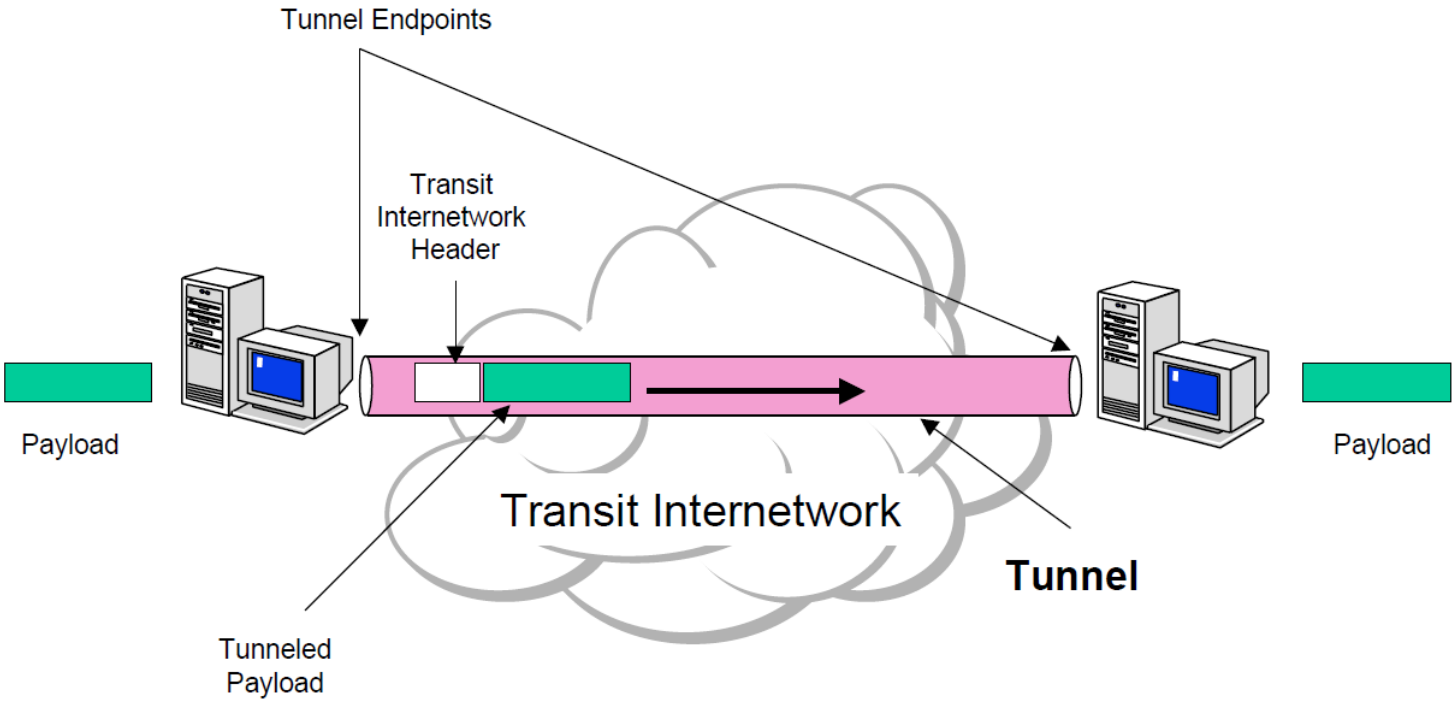


What a VPN needs ?

- VPNs must be encrypted
  - so no one can read it
- VPNs must be authenticated
- No one outside the VPN can alter the VPN
- All parties to the VPN must agree on the security properties

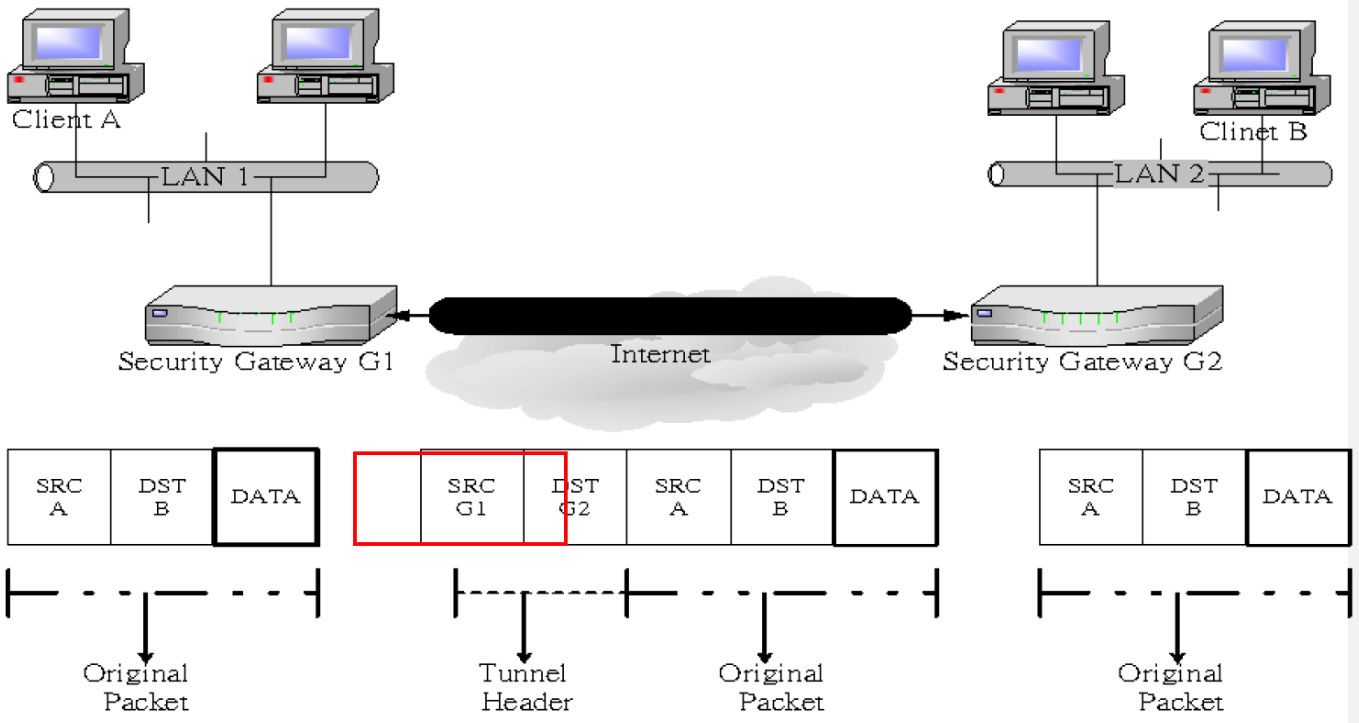
Tunneling

- Core technology
  - VPN consists of a set of point to point connections tunnelled over the Internet



Encapsulation

- In order to achieve tunneling, the packets are encapsulated as the payload of packets
  - Payloads, to and from addresses, port numbers and other standard protocol packet headers
  - As seen by the external routers carrying the connection

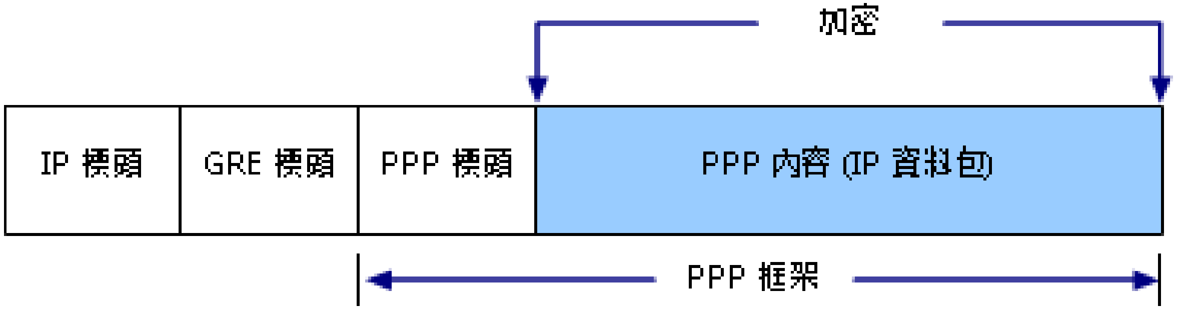


Implementations

- ❑ Point-to-Point Tunneling Protocol (PPTP)
  - RFC 2637
- ❑ Layer 2 Tunneling Protocol (L2TP)
  - RFC 2661
- ❑ IPSec Tunnel Mode
  - RFC 2401
- ❑ Secure Socket Tunneling Protocol (SSTP)

PPTP

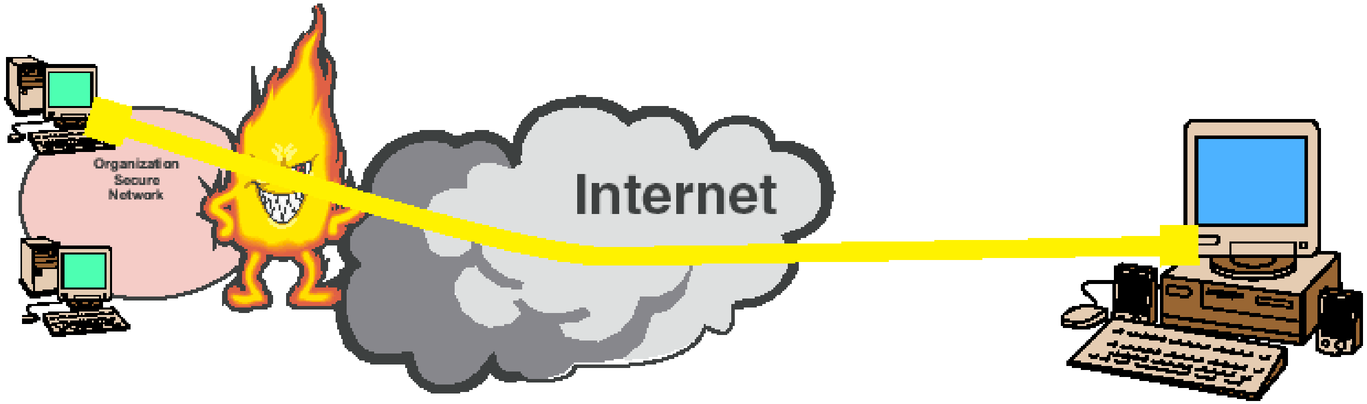
- **Point-to-Point Tunneling Protocol** (PPTP) is a method for implementing VPN
  - PPTP doesn’t describe encryption or authentication
    - Rely on the PPP protocol
  - PPTP was the first VPN protocol that was supported by Microsoft Dial-up Networking
  - Microsoft 2003 and higher also support the PPTP protocol
  - In Microsoft, the tunneled PPP traffic can be authenticated with PAP, CHAP, Microsoft CHAP V1/V2



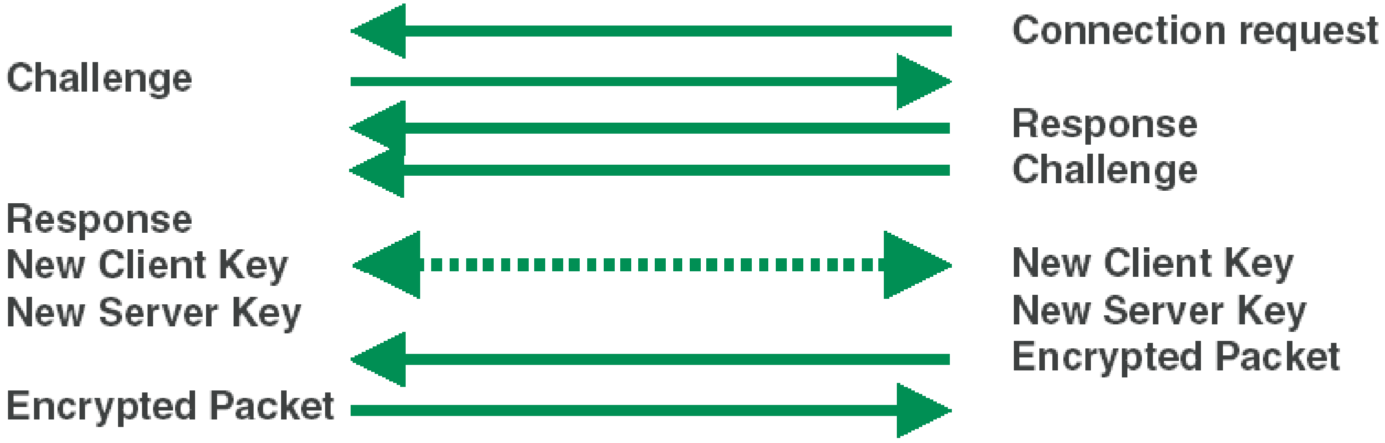
Security of PPTP protocol

- ❑ PPTP has been the subject of many security analyses and serious security vulnerabilities have been found
  - MSCHAP-v1 is fundamentally insecure
  - MSCHAP-v2 is vulnerable to dictionary attack on the captured challenge response packets
- ❑ The PPP payload can be encrypted by using Microsoft Point to Point Encryption (MPPE) when using MSCHAPv1/v2
- ❑ EAP-TLS is the superior authentication choice for PPTP

PPTP: Security



CHAP V2 Authentication with 40 or 128 bit RC4 encryption



Connection request

Challenge

Response
Challenge

Response
New Client Key
New Server Key

New Client Key
New Server Key
Encrypted Packet

Encrypted Packet

mpd

- ❑ Mpd is a netgraph(4) based implementation of the multi-link PPP protocol for FreeBSD
  - /usr/ports/net/mpd5
- ❑ startup
  - vi /etc/rc.conf

```
gateway_enable="YES“
mpd_flags="-b“
mpd_enable="YES"
/usr/local/etc/rc.d/mpd5 {start|stop|restart|rcvar|status}
```

- ❑ Configuration files
  - /usr/local/etc/mpd5/
    - ➢ mpd.conf
    - ➢ mpd.secret

mpd authentication

- /usr/local/etc/mpd5/mpd.secret

```
vpn         “vpn_passwd”         140.113.0.0/16
foo1        “foofoo”             1.2.3.4/32
```

  - plain text
  - chmod 600 mpd.secret

mpd configuration

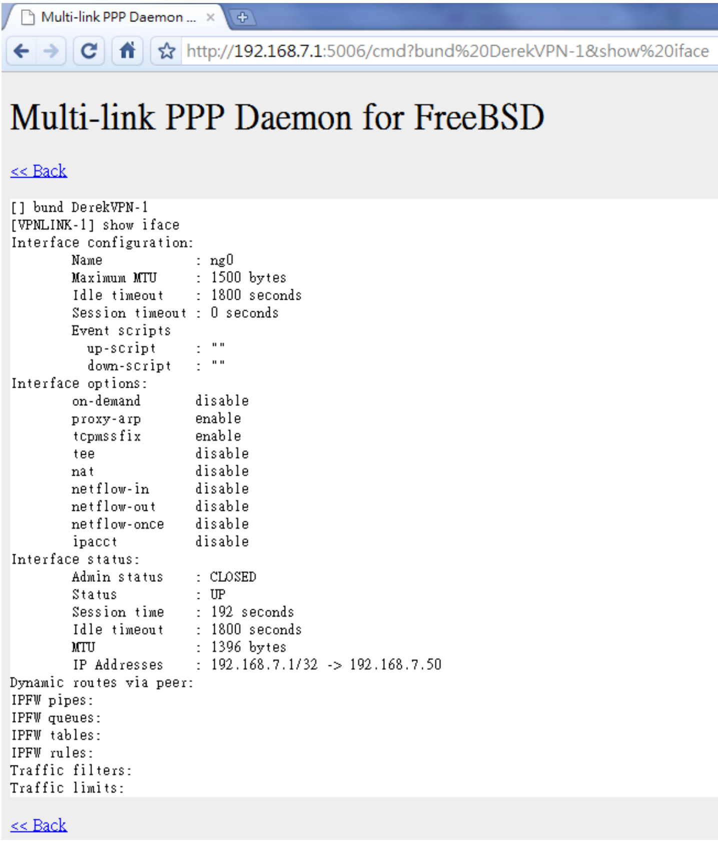
- mpd.conf
  - Consists of a *label* followed by a sequence of mpd commands
  - A label begins at the first column and ends with a colon character
  - Commands are indented with a tab character and follow the label on the next and subsequent lines

```
client:
	create bundle template B1
	create link static L1 modem
	set modem device /dev/cuad0
	set modem speed 115200
	set modem script DialPeer
	set modem idle-script AnswerCall
	set modem var $DialPrefix "DT"
	set modem var $Telephone "1234567"
	set link no pap chap eap
	set link accept pap
	set auth authname "MyLogin"
	set auth password "MyPassword"
	set link max-redial 0
	set link action bundle B1
	open
```

mpd configuration

- startup section
  - Version 4.0b2
    - Added a new startup section to the config-file, wich is loaded once at startup

```
startup:
        # configure mpd users
        set user foo1 bar1
        # configure the console
        set console self 127.0.0.1 5005
        set console open
        # configure the web server
        set web self 0.0.0.0 5006
        set web open
```

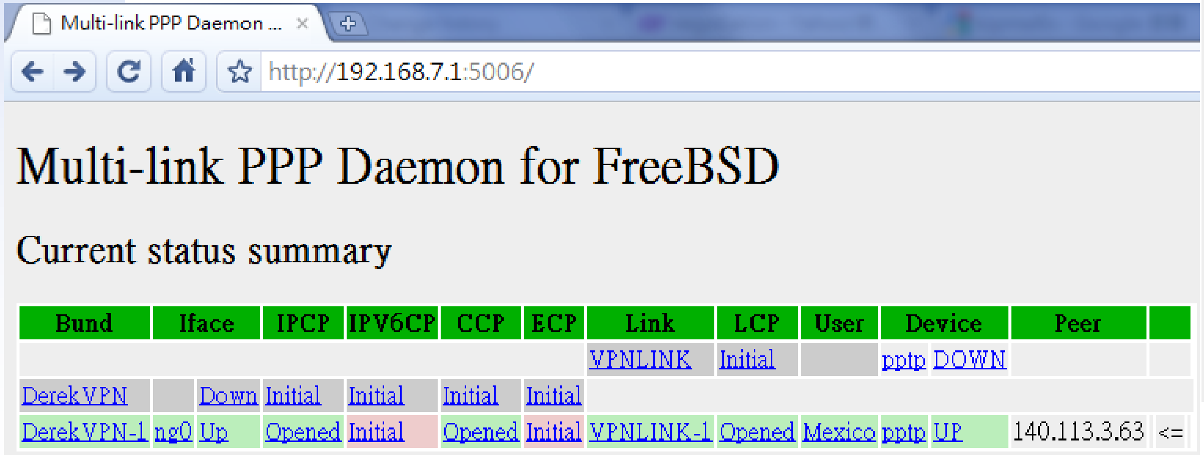

Multi-link PPP Daemon ...
http://192.168.7.1:5006/cmd?bund%20DerekVPN-1&show%20iface

Multi-link PPP Daemon for FreeBSD

<< Back

```
[] bund DerekVPN-1
[VPNLINK-1] show iface
Interface configuration:
        Name            : ng0
        Maximum MTU     : 1500 bytes
        Idle timeout    : 1800 seconds
        Session timeout : 0 seconds
        Event scripts
          up-script     : ""
          down-script   : ""
Interface options:
        on-demand       disable
        proxy-arp       enable
        tcpmssfix       enable
        tee             disable
        nat             disable
        netflow-in      disable
        netflow-out     disable
        netflow-once    disable
        ipacct          disable
Interface status:
        Admin status    : CLOSED
        Status          : UP
        Session time    : 192 seconds
        Idle timeout    : 1800 seconds
        MTU             : 1396 bytes
        IP Addresses    : 192.168.7.1/32 -> 192.168.7.50
Dynamic routes via peer:
IPFW pipes:
IPFW queues:
IPFW tables:
IPFW rules:
Traffic filters:
Traffic limits:
```

<< Back



Multi-link PPP Daemon for FreeBSD

Current status summary

Bund	Iface		IPCP	IPV6CP	CCP	ECP	Link	LCP	User	Device		Peer	
							VPNLINK	Initial		pptp	DOWN		
DerekVPN		Down	Initial	Initial	Initial	Initial							
DerekVPN-1	ng0	Up	Opened	Initial	Opened	Initial	VPNLINK-1	Opened	Mexico	pptp	UP	140.113.3.63	<=

mpd configuration

- ❑ default section
  - Set interface
    - ➢ ip range
  - Set bundle name
  - Link layer configuration

mpd layers

interface -> ipcp -> compression -> encryption -> bundle -> links

```
default:
        load pptp_server

pptp_server:
        # Define dynamic IP address pool.
        set ippool add VPNPOOL 192.168.1.50 192.168.1.99
        # Create clonable bundle template
        create bundle template VPN

        set iface enable proxy-arp
        set iface idle 1800
        set iface enable tcpmssfix  # adjust incoming and outgoing TCP SYN segments (MTU)
        set ipcp yes vjcomp      # Van Jacobson TCP header compression
        # Specify IP address pool for dynamic assigment.
        set ipcp ranges 192.168.1.1/32 ippool VPNPOOL
```

mpd configuration

- default section
  - Link layer configuration

```
pptp_server:
            …. (skip)
            # Create clonable link template named L
            create link template VPNLINK pptp
            # Set bundle template to use
            set link action bundle VPN
            # Multilink adds some overhead, but gives full 1500 MTU.
            set link enable multilink
            # Address and control field compression, save 2 bytes,
            # Protocol field compression, save 1 byte
            set link yes acfcomp protocomp
            set link keep-alive 10 60

            # Configure PPTP
            set pptp self 1.2.3.4
            set link enable incoming
```

Encryption

- Microsoft Point-to-point compression (MPPC) CCP subprotol
  - 'mppc' option should be enabled at the CCP layer

```
# The five lines below enable Microsoft Point-to-Point encryption
# (MPPE) using the ng_mppc(8) netgraph node type.
    set bundle enable compression
    set ccp yes mppc
    set mppc yes e40
    set mppc yes e128
    set mppc yes stateless
```

mpd configuration

- Minimum configuration

```
startup:
default:
                set ippool add VPNPOOL 192.168.1.11 192.168.1.15
                create bundle template NAVPN
                set ipcp ranges 192.168.1.1/32 ippool VPNPOOL
                create link template VPNLINK pptp
                set link action bundle NAVPN
                set link no pap chap eap
                set link enable chap-msv2
                set pptp self 1.2.3.4
                set link enable incoming
```

http://mpd.sourceforge.net/doc5/mpd.html

syslog

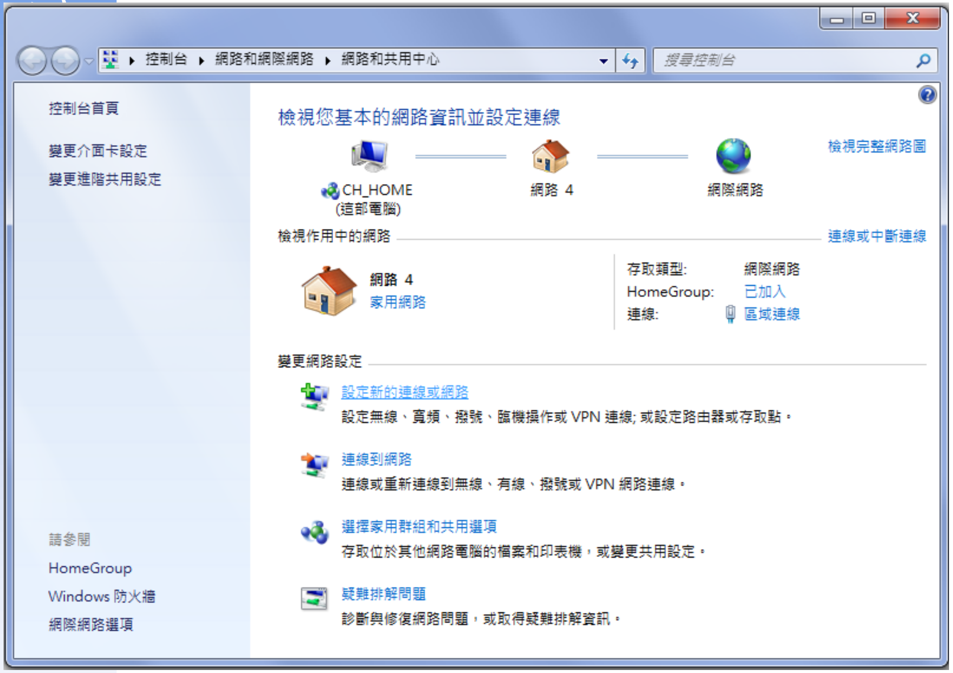
- Modify /etc/syslog.conf

```
!mpd
*.*                         /var/log/mpd.log
```

- touch /var/log/mpd.log
- /etc/rc.d/syslogd reload

VPN client

- ❑ 建立新的連線



控制台 ▸ 網路和網際網路 ▸ 網路和共用中心

搜尋控制台

控制台首頁

變更介面卡設定

變更進階共用設定

檢視您基本的網路資訊並設定連線

檢視完整網路圖

CH_HOME (這部電腦) — 網路 4 — 網際網路

檢視作用中的網路

連線或中斷連線

網路 4
家用網路

存取類型: 網際網路
HomeGroup: 已加入
連線: 區域連線

變更網路設定

設定新的連線或網路
設定無線、寬頻、撥號、臨機操作或 VPN 連線; 或設定路由器或存取點。

連線到網路
連線或重新連線到無線、有線、撥號或 VPN 網路連線。

選擇家用群組和共用選項
存取位於其他網路電腦的檔案和印表機，或變更共用設定。

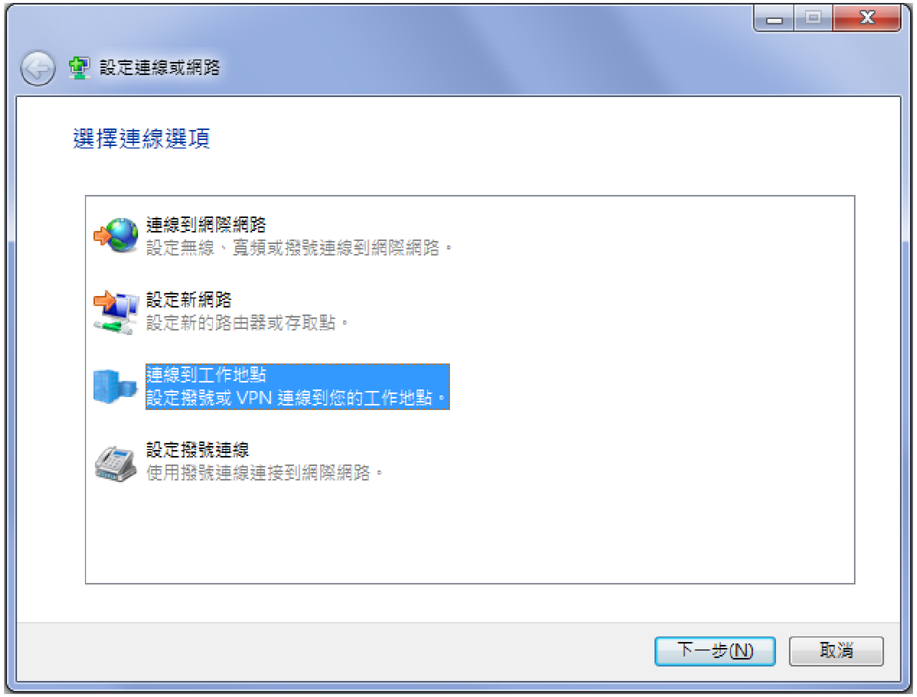
疑難排解問題
診斷與修復網路問題，或取得疑難排解資訊。

請參閱

HomeGroup

Windows 防火牆

網際網路選項



設定連線或網路

選擇連線選項

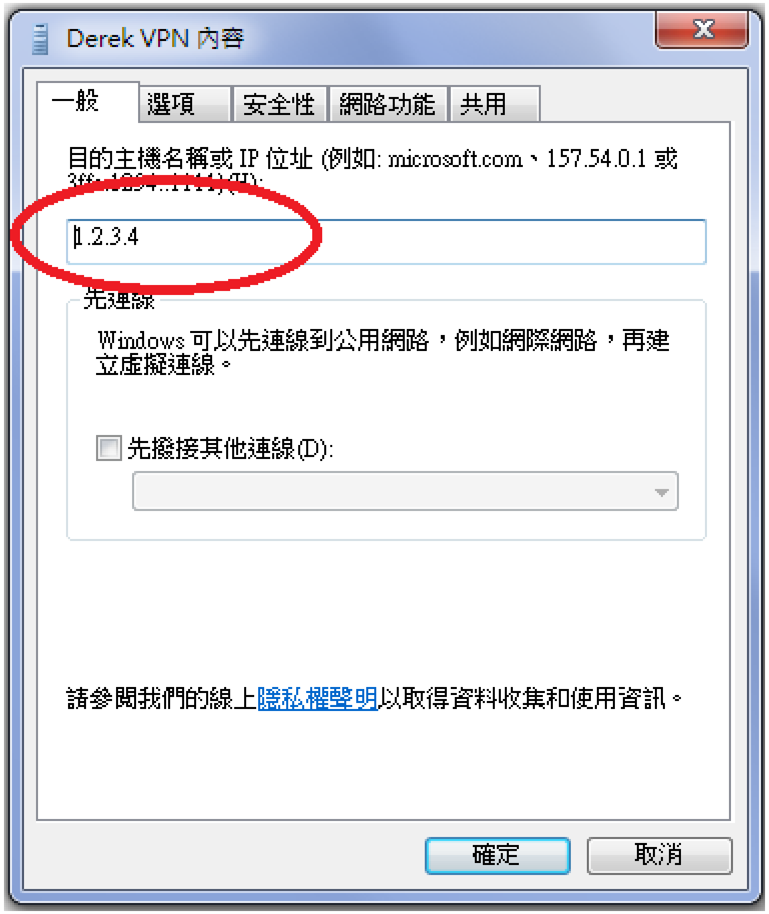
連線到網際網路
設定無線、寬頻或撥號連線到網際網路。

設定新網路
設定新的路由器或存取點。

連線到工作地點
設定撥號或 VPN 連線到您的工作地點。

設定撥號連線
使用撥號連線連接到網際網路。

VPN client



Derek VPN 內容

一般 | 選項 | 安全性 | 網路功能 | 共用

目的主機名稱或 IP 位址 (例如: microsoft.com、157.54.0.1 或 3ffe:1234::1111)(T):

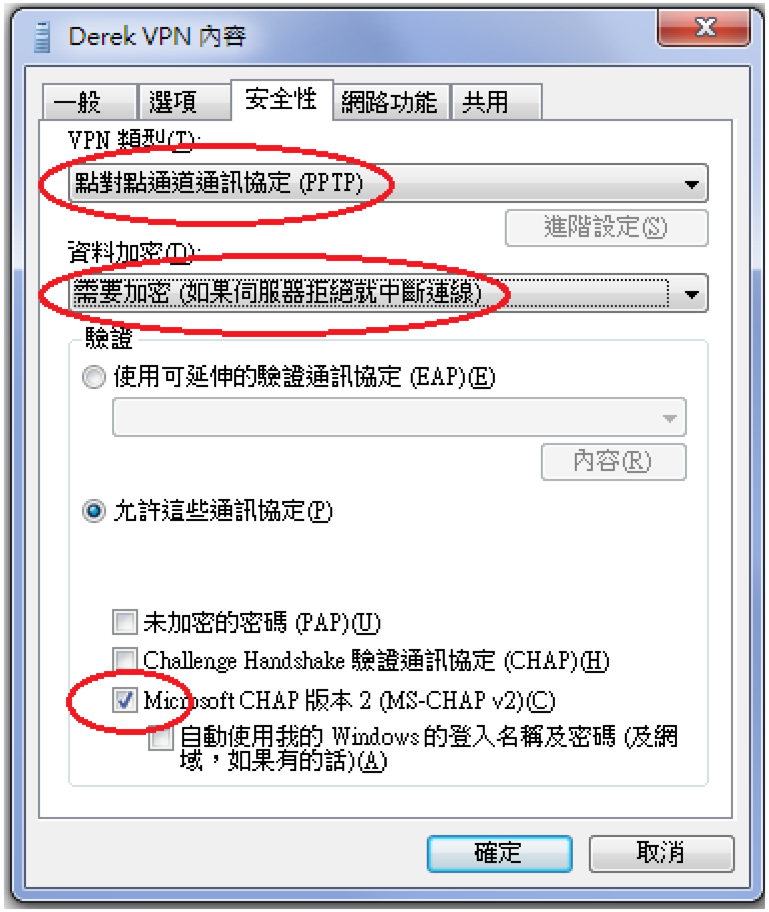
1.2.3.4

先連線

Windows 可以先連線到公用網路，例如網際網路，再建立虛擬連線。

□ 先撥接其他連線(D):

請參閱我們的線上隱私權聲明以取得資料收集和使用資訊。



Derek VPN 內容

一般 | 選項 | 安全性 | 網路功能 | 共用

VPN 類型(T):

點對點通道通訊協定 (PPTP)

資料加密(D):

需要加密 (如果伺服器拒絕就中斷連線)

驗證

○ 使用可延伸的驗證通訊協定 (EAP)(E)

● 允許這些通訊協定(P)

□ 未加密的密碼 (PAP)(U)

□ Challenge Handshake 驗證通訊協定 (CHAP)(H)

☑ Microsoft CHAP 版本 2 (MS-CHAP v2)(C)

□ 自動使用我的 Windows 的登入名稱及密碼 (及網域，如果有的話)(A)