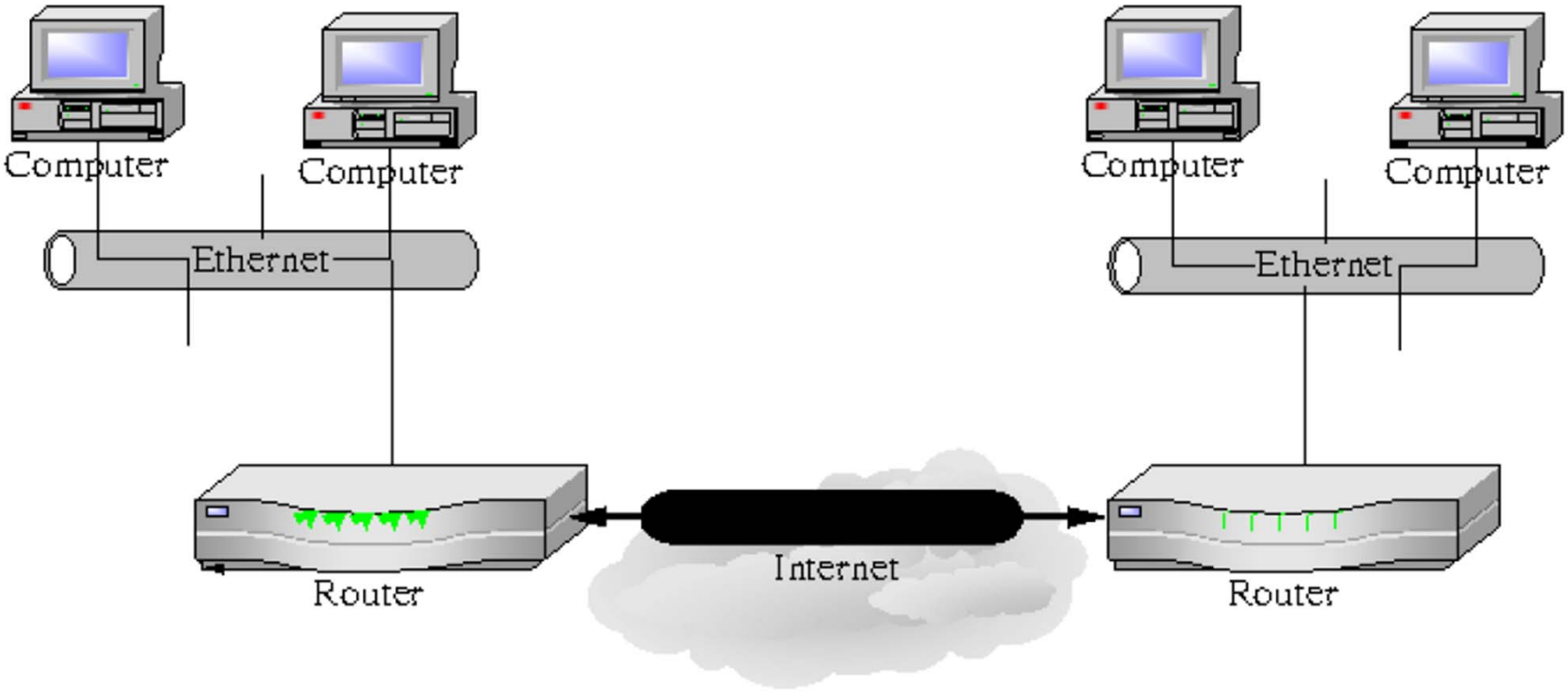
Virtual Private Network

pmli

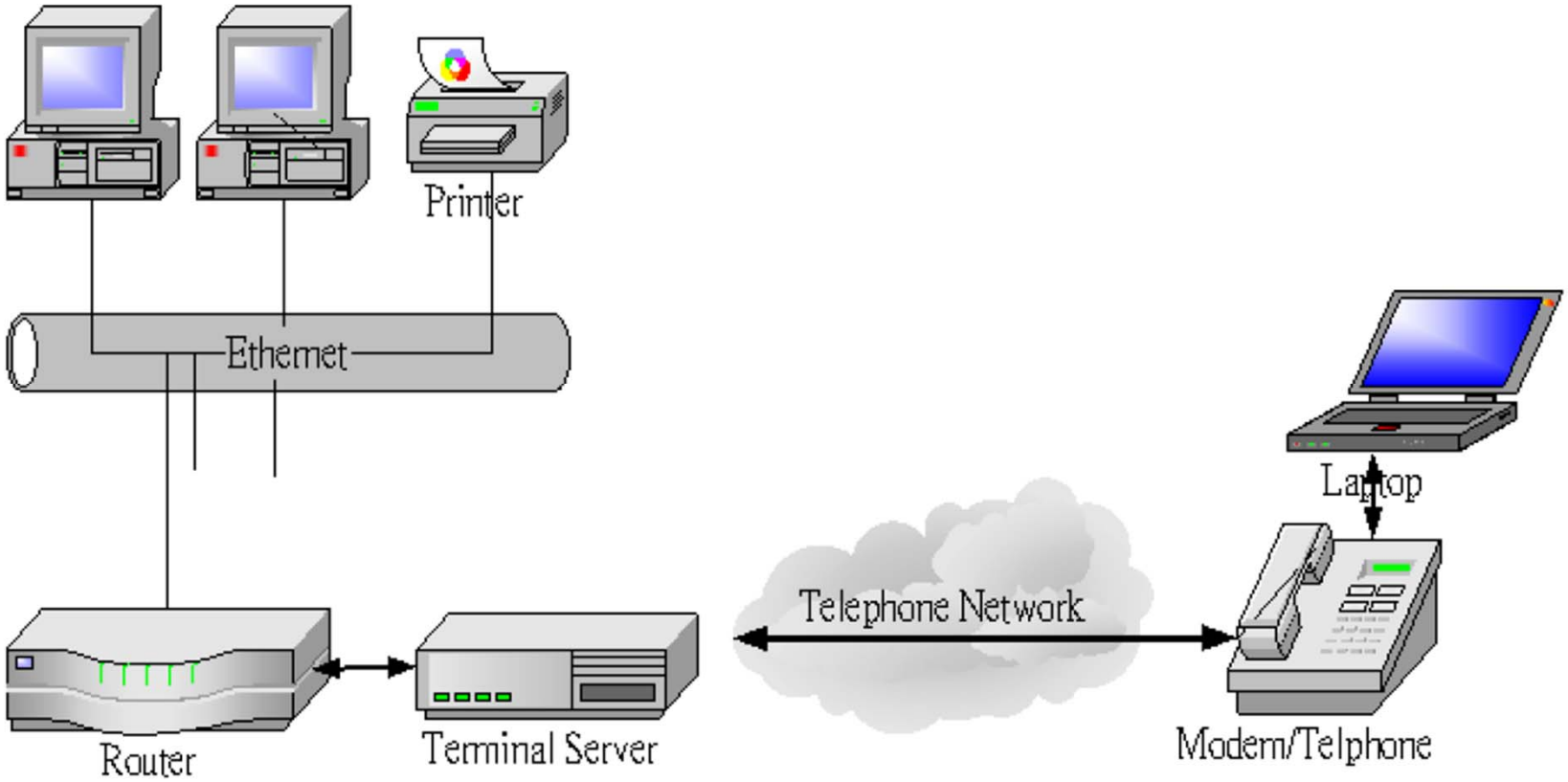
What is a VPN

- Used to connect two private networks together via the Internet



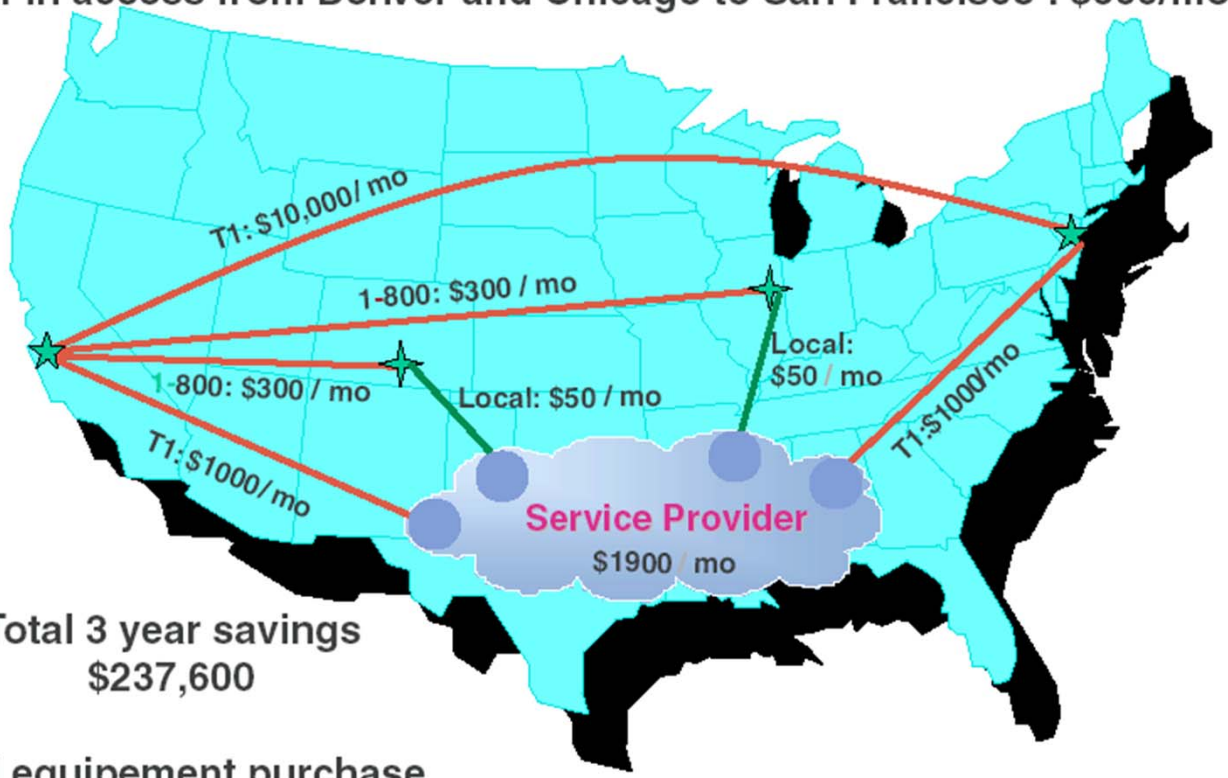
What is a VPN

- 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

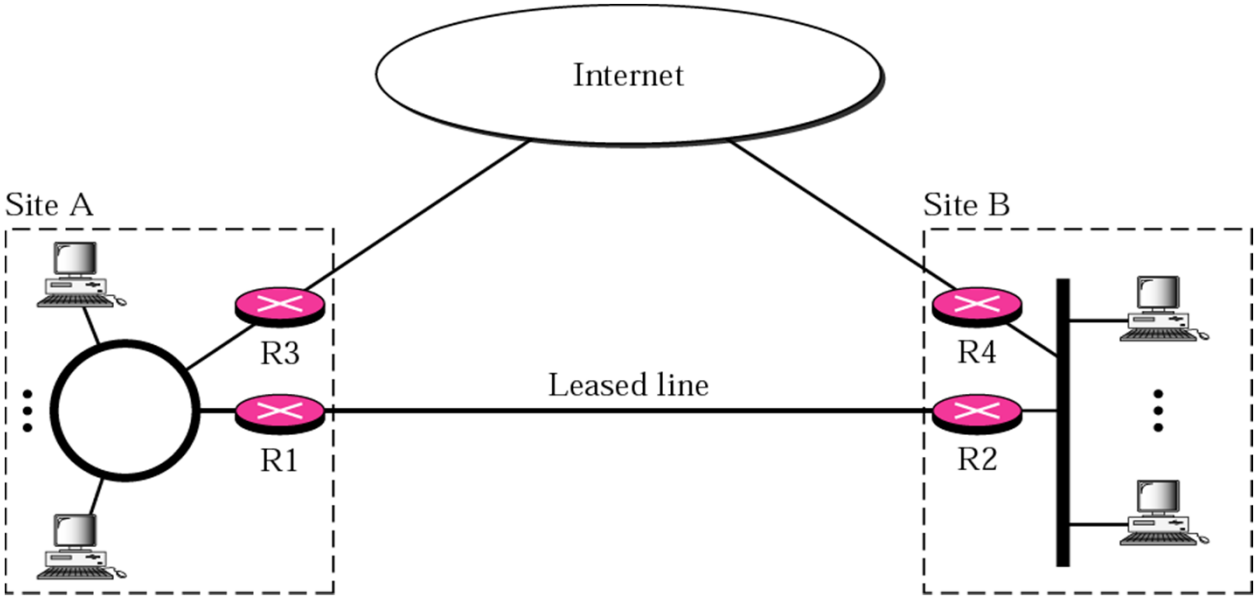


Total 3 year savings
$237,600

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

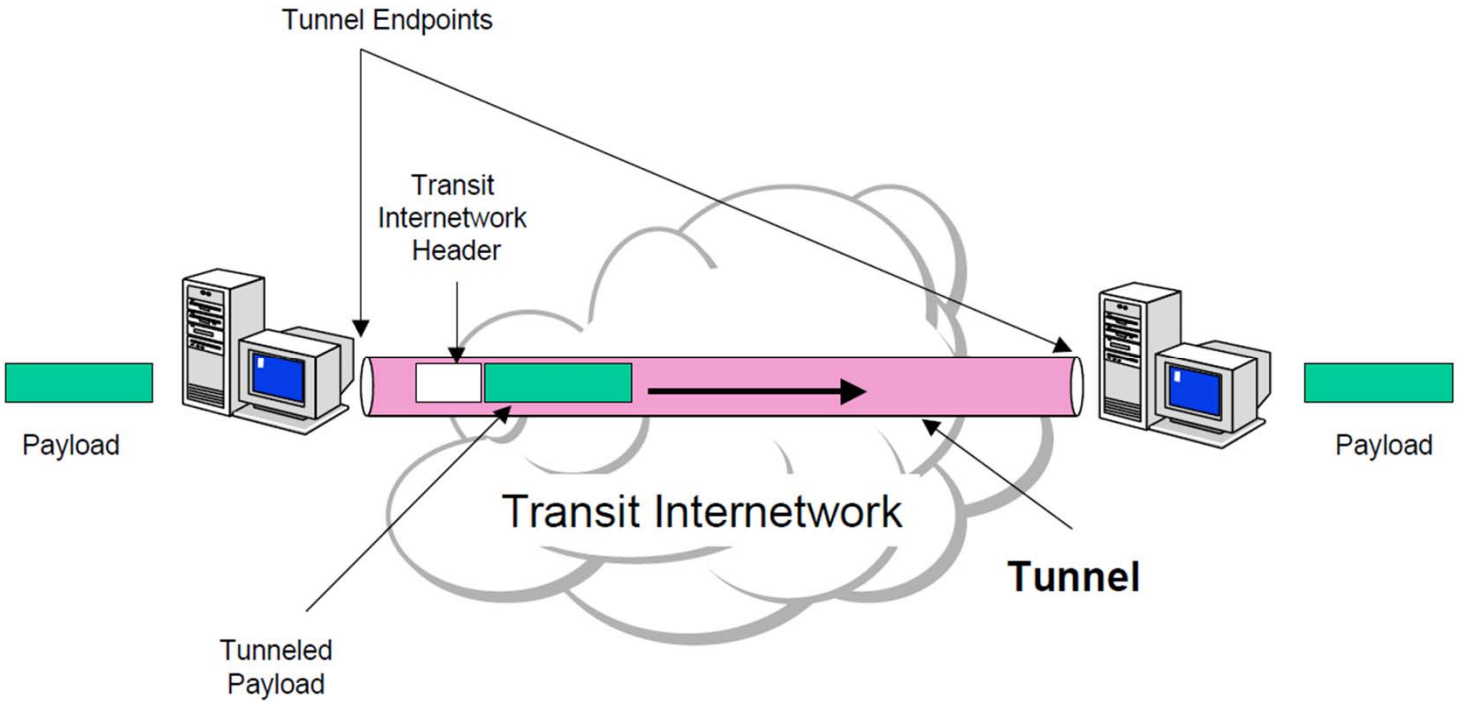


What a VPN needs ?

- 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

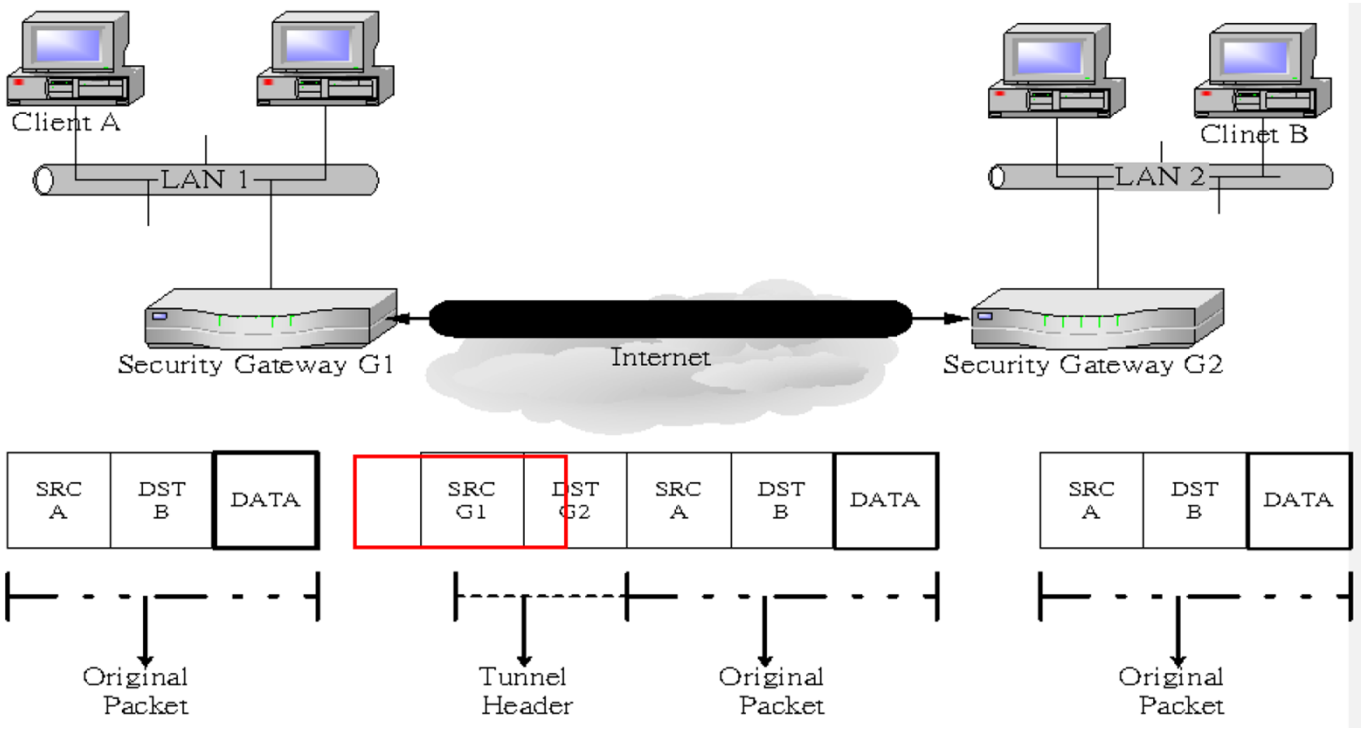
Tunneling

- 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

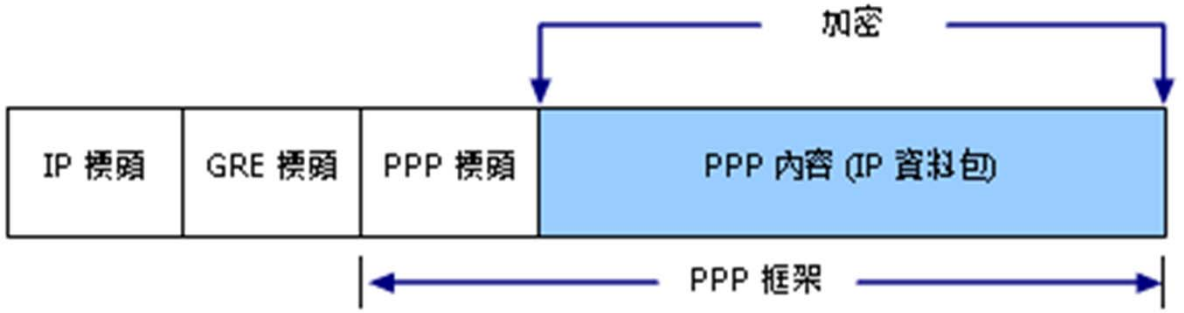


Implementations

- 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

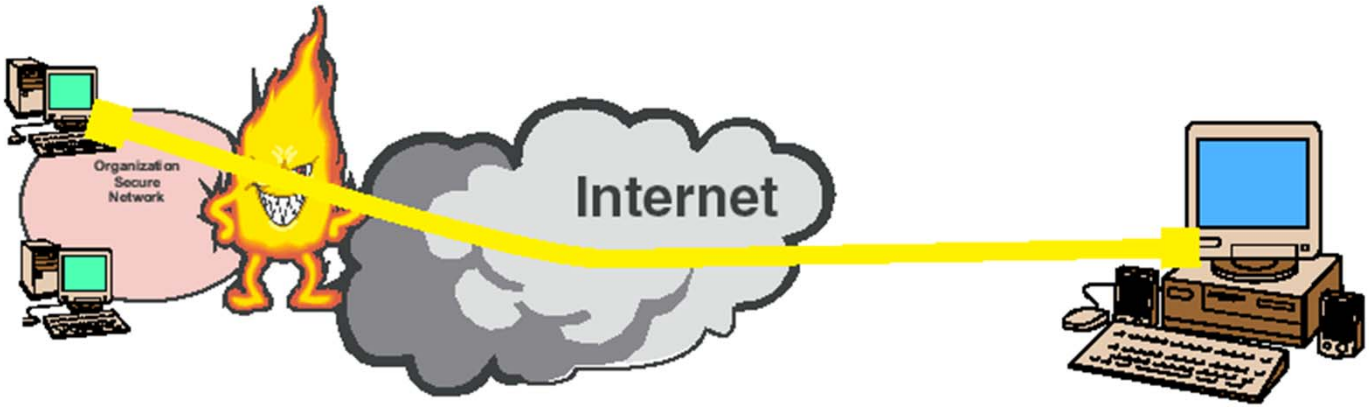
- **Point-to-Point Tunneling Protocol** (PPTP) is a method for implementing VPN
  - PPTP doesn't describe encryption or authentication
    - Rely on the PPP protocol
  - PPTP was the first VPN protocol that was supported by Microsoft Dial-up Networking
  - Microsoft 2003 and higher also support the PPTP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



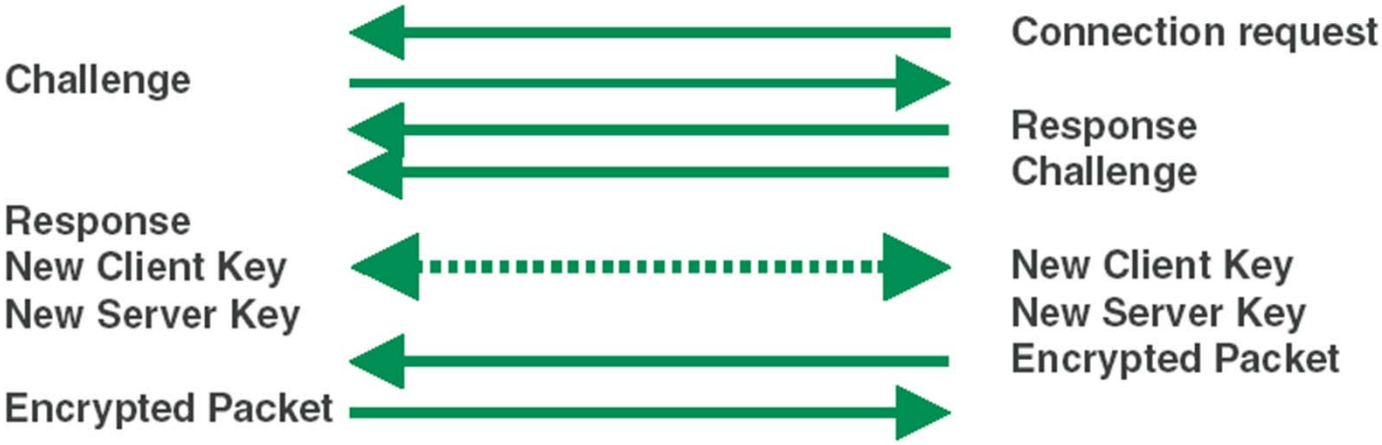
Security of PPTP protocol

- 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



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

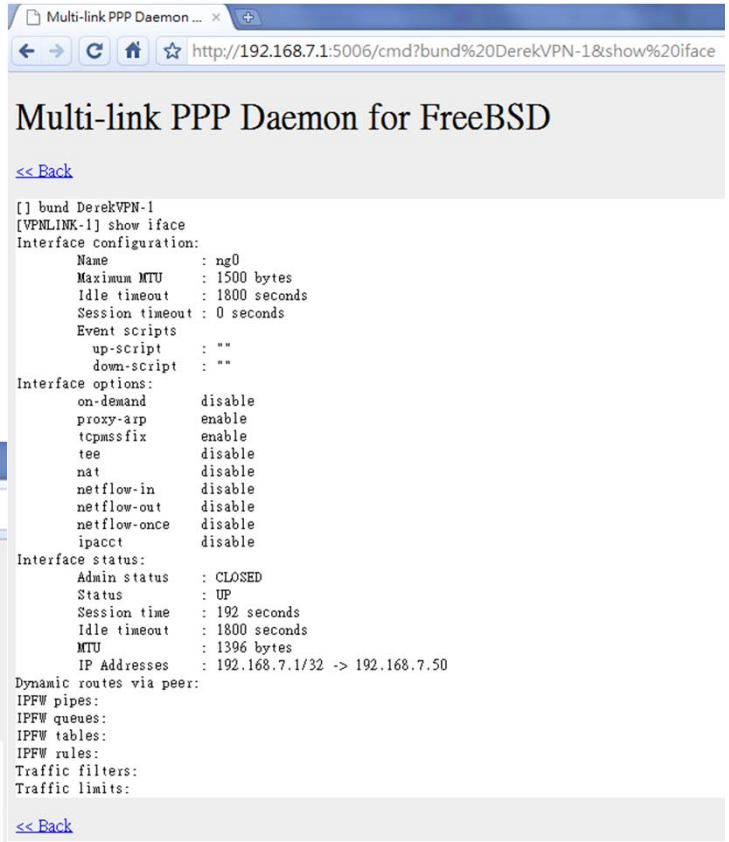
- mpd.conf
  - Consists of a *label* followed by a sequence of mpd commands
  - A label begins at the first column and ends with a colon character
  - Commands are indented with a tab character and follow the label on the next and subsequent lines

```
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
```



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

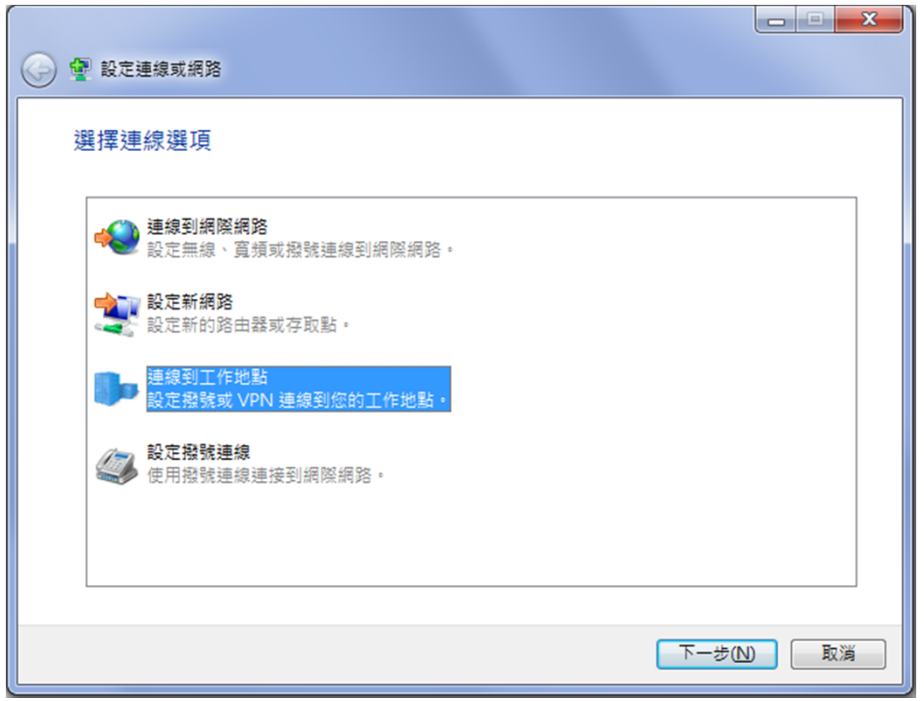
- Modify /etc/syslog.conf

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

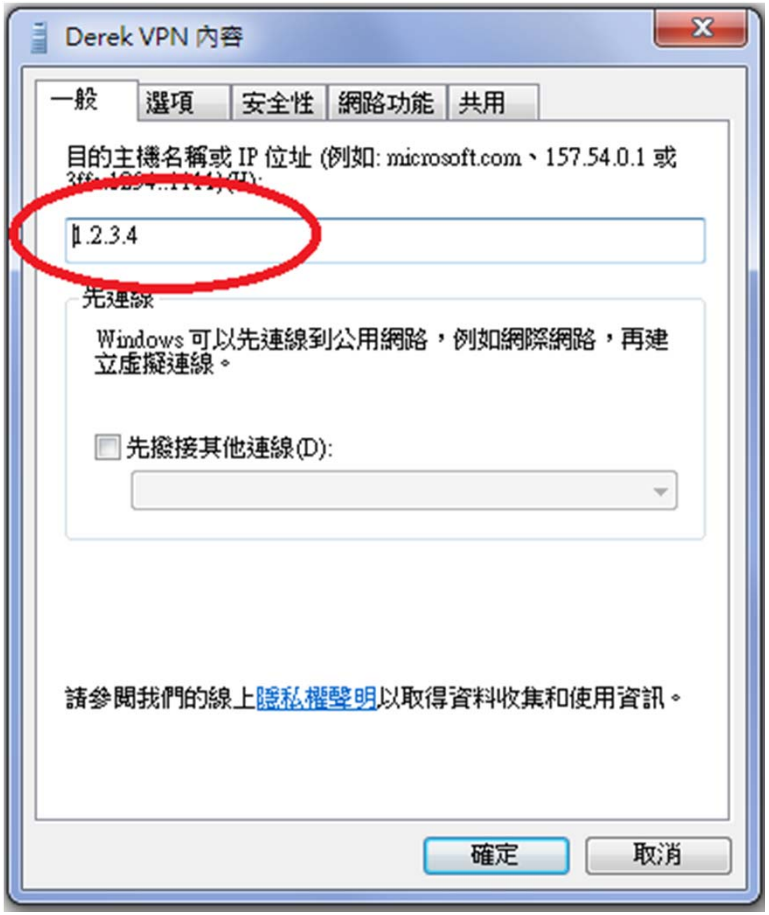
- touch /var/log/mpd.log
- /etc/rc.d/syslogd reload

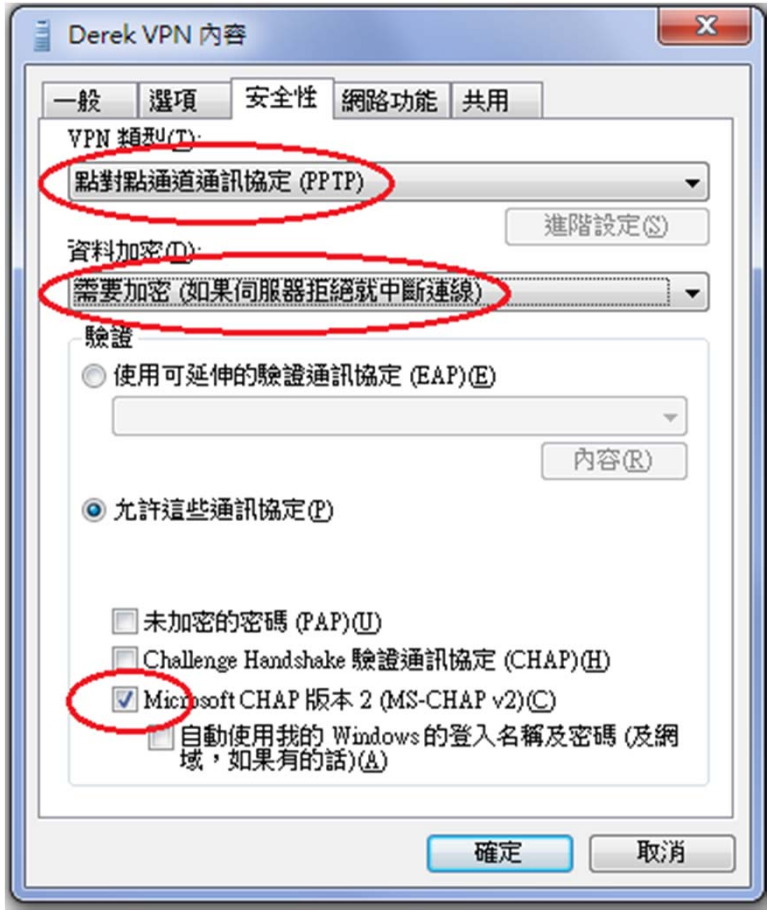
VPN client

- 建立新的連線



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
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。
確定
取消


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)
進階設定(S)
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)
內容(R)
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)
確定
取消