VPN 虛擬私有網路技術概說

李倫銓　講師

CISSP、 BS 7799 LA

課程大綱

- 第一章 VPN 概述
- 第二章 VPN 技術介紹
- 第三章 VPN 的應用與風險簡述
- 第四章 結論

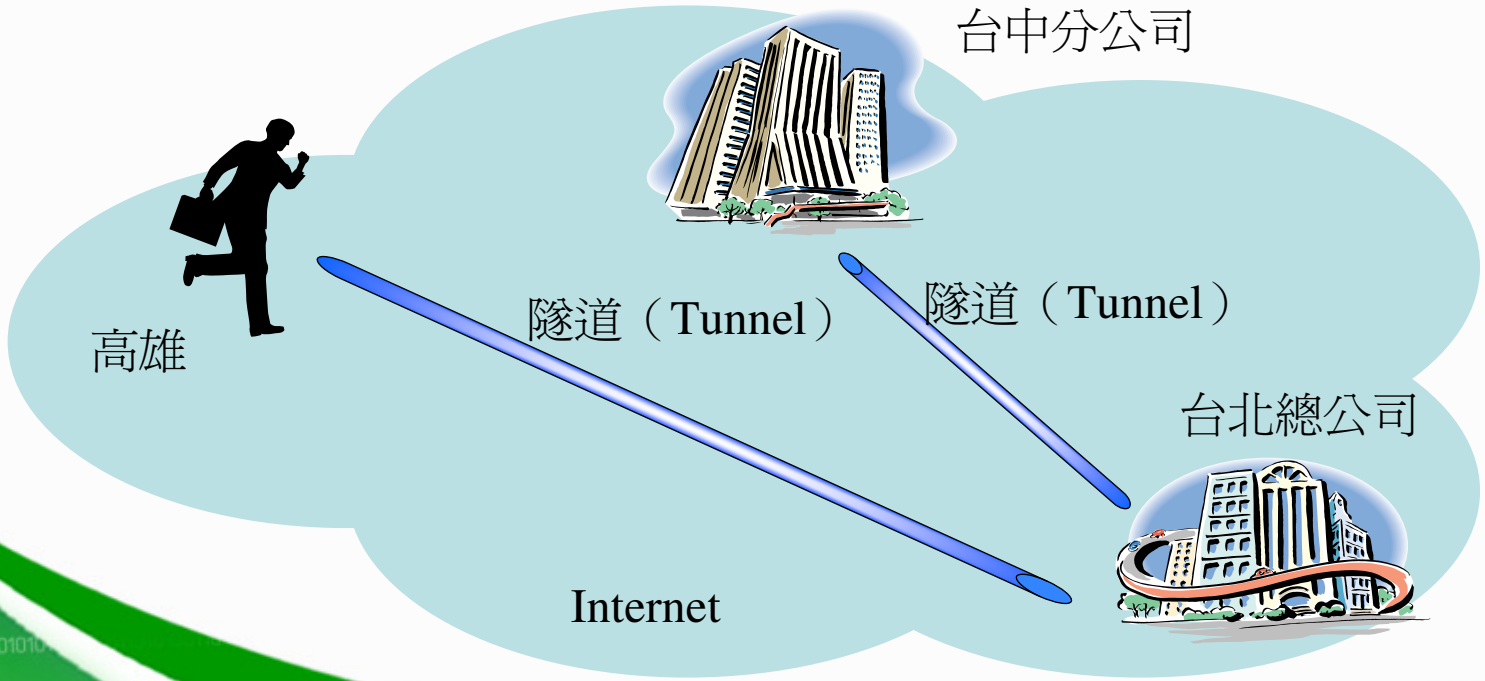
第一章 VPN 概述

- 1-1 何謂 VPN
- 1-2 VPN 種類
- 1-3 VPN 組成條件

1-1 何謂 VPN

VPN 虛擬私有網路

- VPN 虛擬私有網路（Virtual Private Network）
  - 利用穿隧（Tunneling）技術、加解密等安全技術，在公眾網路（例如Internet）上，建構出虛擬的私有網路（Private Network），以達到私有網路的安全與便利性。



虛擬與穿隧

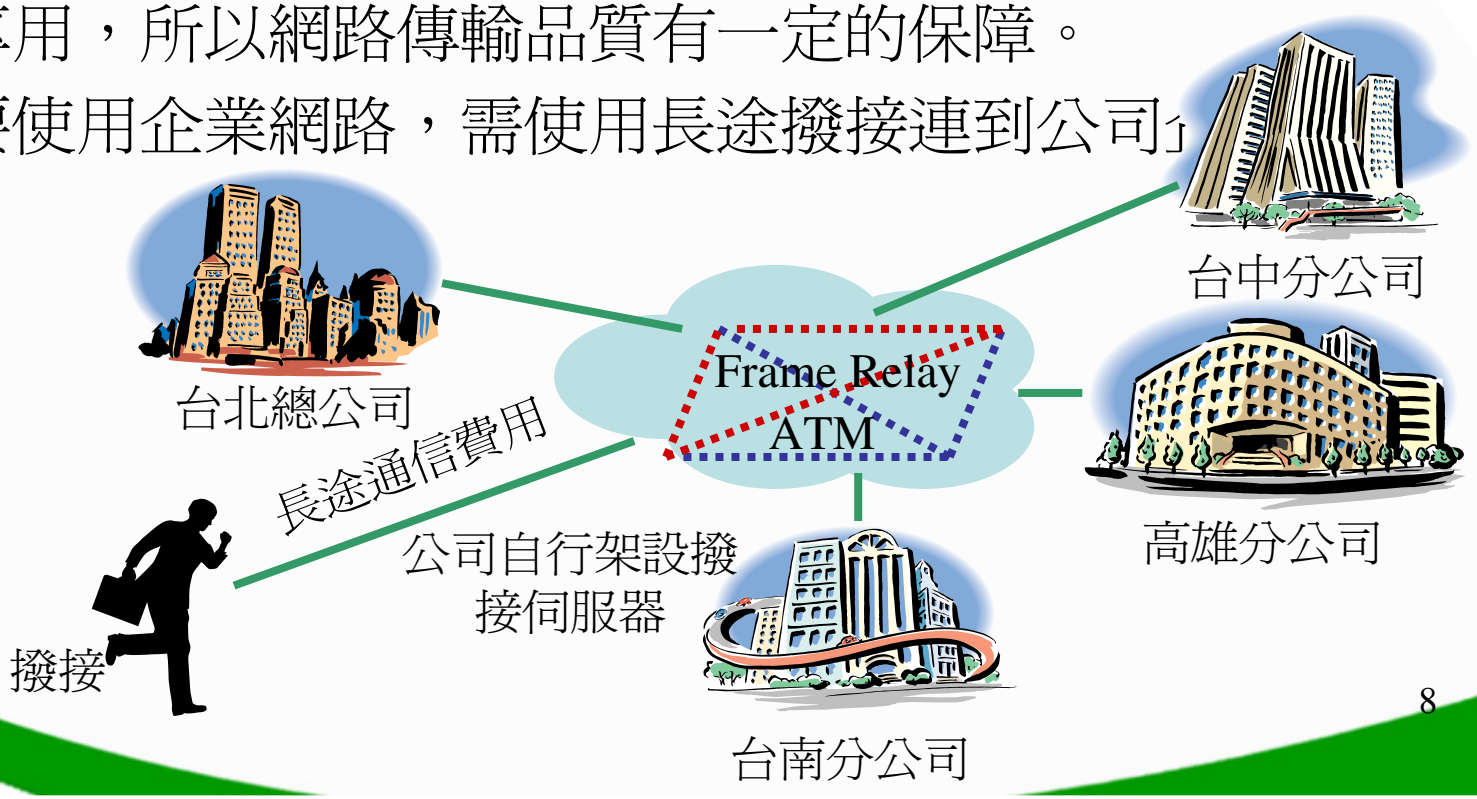
- 何謂「虛擬」?
  - 虛擬是指此隧道並非實體上有專門的線路連接，而是利用通信協定的技術所形成。
- 何謂「穿隧」?
  - 穿隧（Tunneling）技術即是設法在兩個網路間或遠端使用者與內部網路間建立一個虛擬隧道，跨越網際網路。

爲何需要使用 VPN 技術

- 使用VPN可以以公眾網路的便宜價格，享受專屬線路的安全。
- 遠端使用者可藉由ISP提供的撥接網路，不需長途撥接費用，即可安全的連進公司內網。
- 具備資料加密、確保資料完整性 。

傳統私有網路

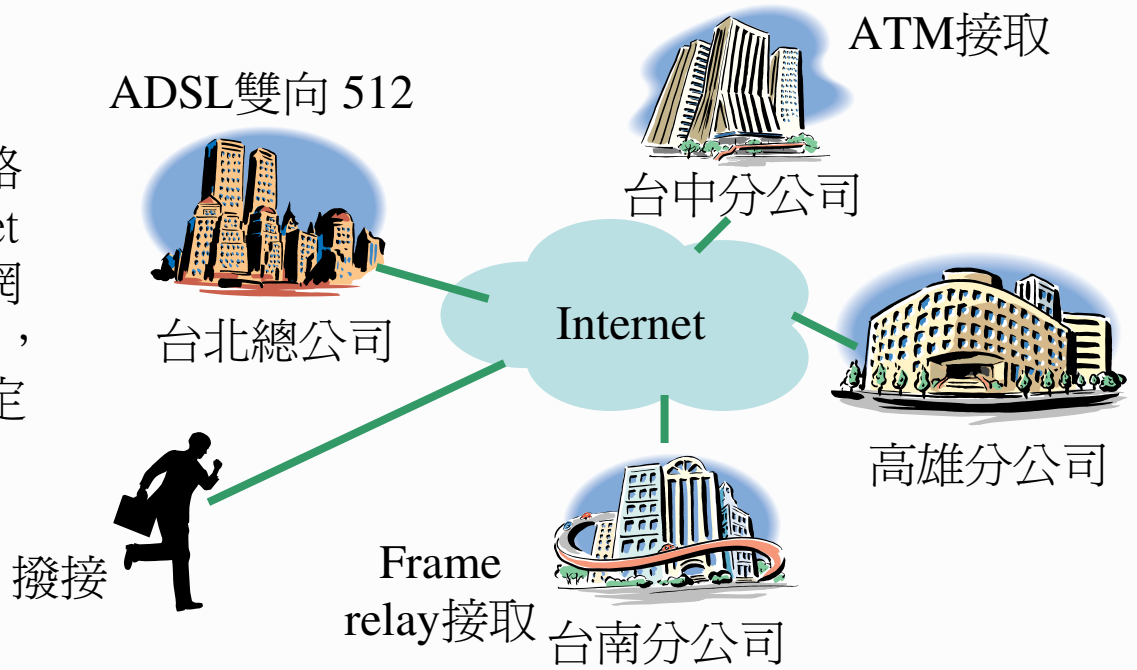
- 由訊框傳送（Frame Relay）或非同步傳輸模式（ATM, Asynchronous Transfer Mode）等技術，提供固定虛擬線路（PVC, Permanent Virtual Connection ）來連接各點。
- 專線專用，所以網路傳輸品質有一定的保障。
- 業務要使用企業網路，需使用長途撥接連到公司網路。



虛擬私有網路

- 企業可利用現有網路接取方式，訂做屬於自己的專屬網路，並不需受限於傳統專線接取點位置。
- 目前各大ISP已提供VPN服務，企業不需自行設定自己VPN網路。

備註：虛擬私有網路指的是建構在Internet上的企業專用私有網路，而非Frame relay，ATM等所提供之固定虛擬線路（PVC）。



VPN 的優點

- 應用更靈活
  - 可使用已有之連線技術（如：ADSL、Cable modem、Frame Relay、ATM）
- 具有較佳的擴充性
  - 擴點容易
  - 更易依需求增加連線頻寬
- 花費較低廉
  - 設備投資成本較低
  - 管理維護簡便

虛擬私有網路與傳統私有網路的差異

	虛擬私有網路	傳統私有網路
通訊與設備費用	低，使用網際網路 勝	高，使用專線，設備投資成本高。
安全性	高，使用加密技術 平	高，專有線路 平
通訊品質	取決於 ISP 的提供的線路品質以及線路擁塞程度	使用專線擁有專屬頻寬 勝
擴充性	具彈性 勝	架構調整，與擴充彈性較差。
管理	管理與維護都方便 涵蓋範圍廣 勝	管理與維護較爲不便，備援性較差。

目前已有提供頻寬保證且便宜的 VPN 服務了！

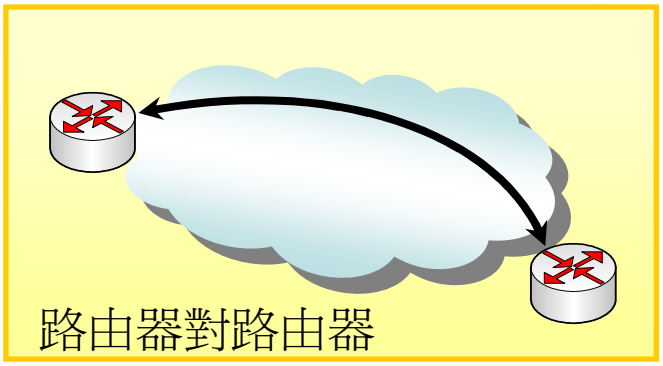
VPN 服務

- 目前國內各大ISP都有提供相關的VPN服務，企業不必自行規劃VPN連線。
  - 目前已整合多種網路接取方式（例如：Frame Relay、ATM、ADSL等），企業可選擇符合自己需求來連結自己的網路。
  - ADSL+VPN服務所構成的企業VPN環境，不但享有ADSL的經濟費率，亦提供同樣的私密與安全性。

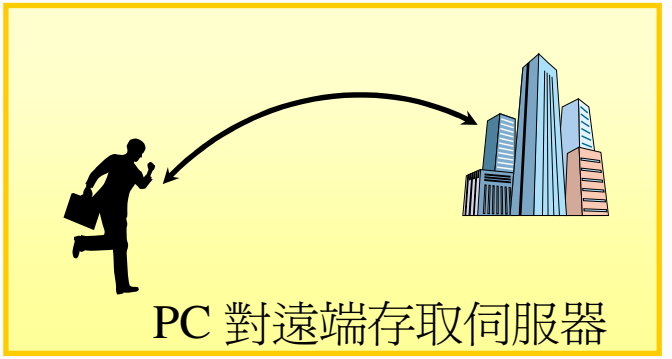
1-2 VPN 種類

依使用方式來分類

- 區網互連型 VPN
  - 如大企業中，子公司之間可互相連接。



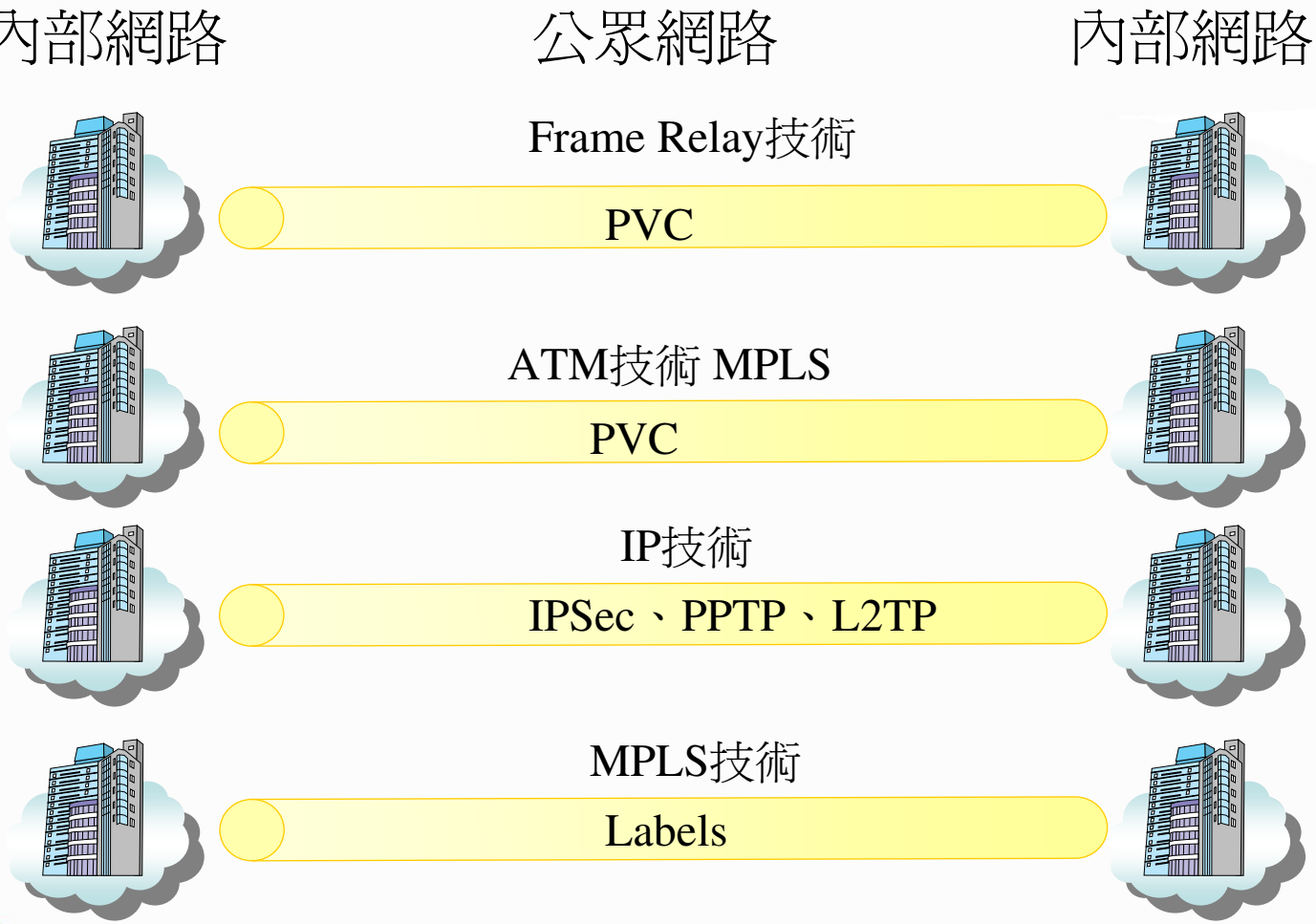
- 遠端存取型 VPN
  - 提供業務在外仍可安全使用公司內部網路。



依據建置單位來區分

- 客戶端設備 VPN
  （CPE -Based VPN, Customer Premises Equipment-Based VPN）
  - L2TP協定、PPTP協定
  - IPSec協定
  - GRE 封裝方式
- 網路提供者提供VPN服務
  （Provider-Based VPN或稱Network-Based VPN）
  - OSI第二層VPN：Frame relay、ATM
  - MPLS技術

依據建立技術來分類


內部網路
公眾網路
內部網路
Frame Relay技術
PVC
ATM技術 MPLS
PVC
IP技術
IPSec、PPTP、L2TP
MPLS技術
Labels

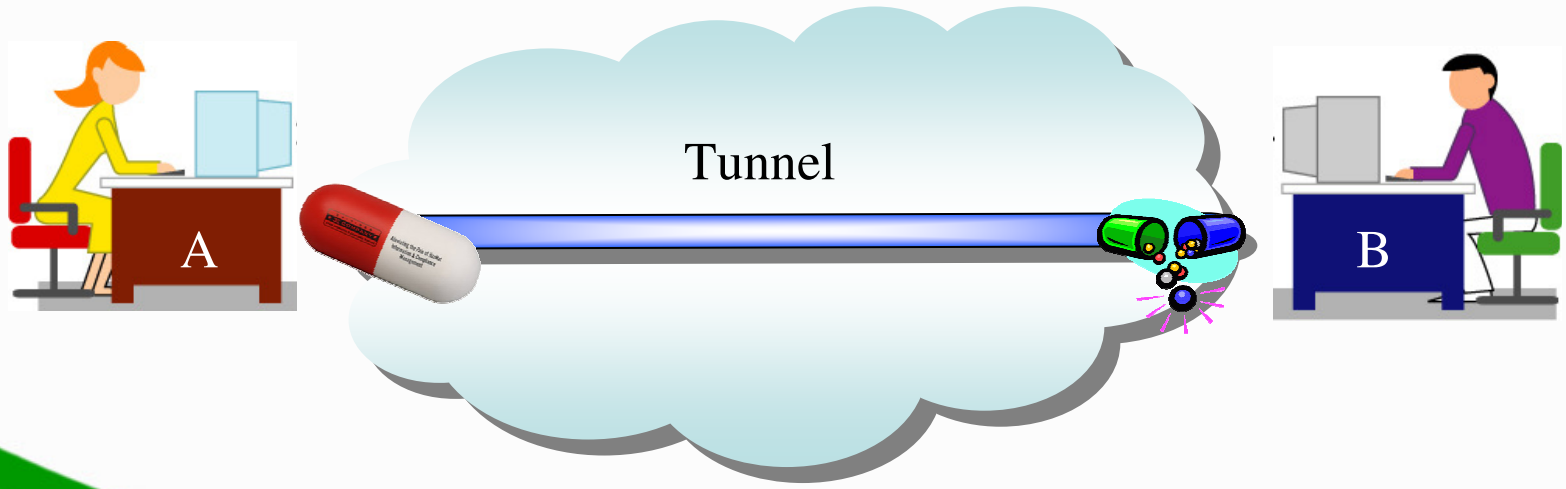
1-3 VPN 組成條件

VPN 主要採用四項原理技術

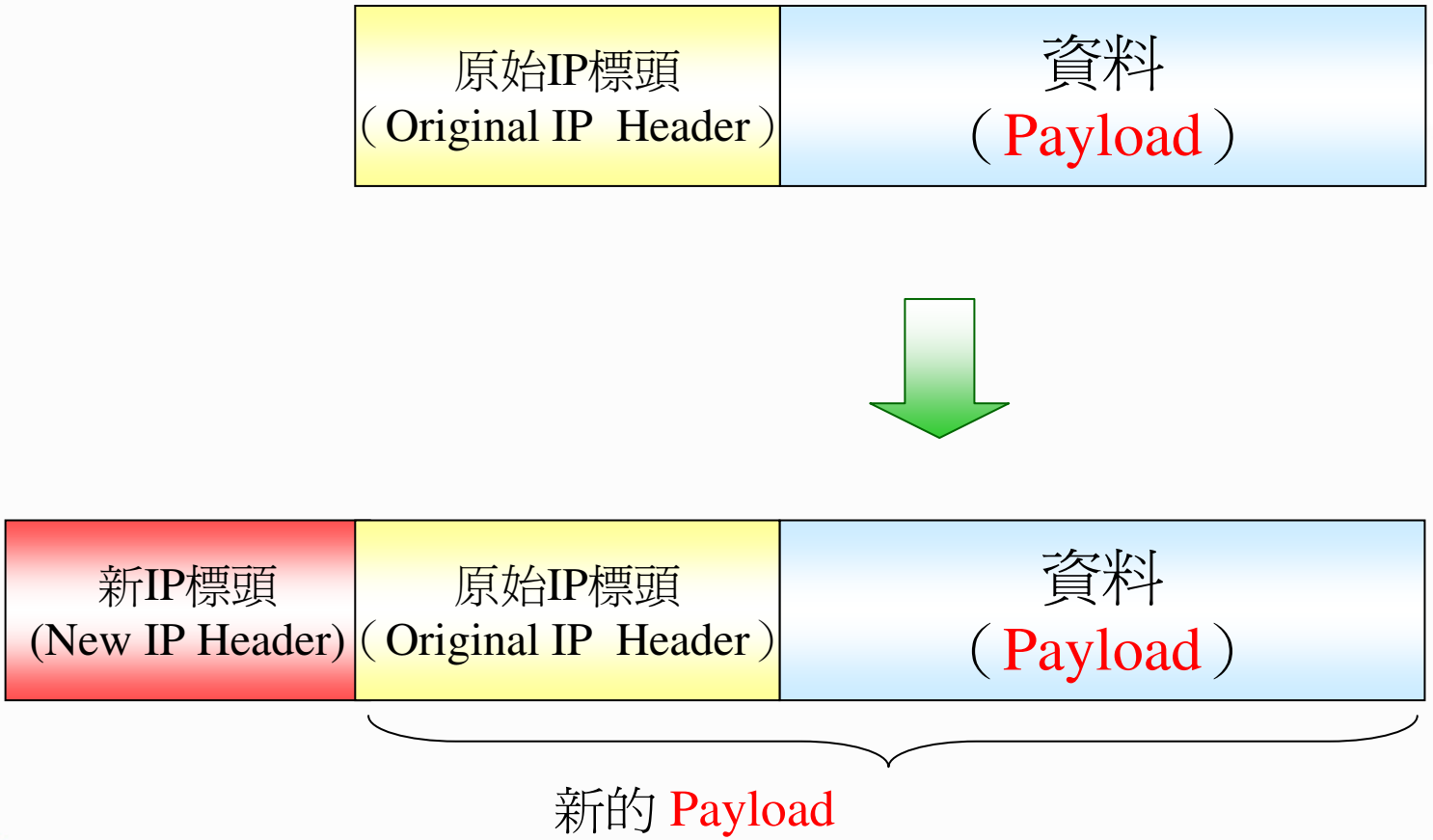
- 穿隧技術（Tunneling）
- 加解密技術（Encryption & Decryption）
- 金鑰管理技術（Key management）
- 使用者與設備身分鑑別技術（Authentication）

Tunneling 穿隧技術

- 穿隧技術就是在 A、B 兩個網路之間建立一個網路連線，這個連線會將 A 網路裡的封包包在這個網路連線的封包裡送到 B，等封包送到 B 網路後再將其解開，恢復成原來的樣子。



Tunneling 穿隧技術



加解密技術
（Encryption & Decryption）

- VPN節點之間，使用DES或3DES這類對稱式加密法對隧道內容加密，才能擁有較快的傳輸效能。
- VPN靠著使用非對稱式密碼技術來做身分確認或金鑰交換。

金鑰管理技術（Key management）

- 由於 VPN 節點間，仍需依靠金鑰管理技術來交換傳輸金鑰。
  - SKIP（Simple Key Management for IP）技術
    - 由SUN發展，主要利用Diffie - Hellman演算法。
  - ISAKMP/Oakley 技術
    - Oakley定義如何分辨及確認金鑰，ISAKMP定義分配金鑰的方法，亦爲將來IPv6與IPSEC的金鑰管理技術。

使用者與設備身分鑑別技術（Authentication）

- 使用者身分鑑別部分：
  - 使用者名稱與密碼、IC 卡鑑別、one-time password
- 設備身分鑑別部分：
  - CA 的 X.509 憑證
  - 分享金鑰（Pre-share key）

第二章 VPN 協定技術

- 2-1 VPN 協定技術介紹
- 2-2 PPTP協定
- 2-3 L2TP 協定
- 2-4 IPSEC 協定
- 2-5 MPLS 技術
- 2-6 SSL VPN 技術
- 2-7 各項協定技術比較

2-1 VPN 協定技術介紹

常見之VPN協定技術與其應用範圍

- 常見的五種VPN協定技術：
  - PPTP協定
  - L2TP協定
  - IPSEC協定
  - MPLS技術
  - SSL VPN技術
- 其中PPTP、L2TP皆爲第二層VPN協定，而IPSEC爲第三層VPN協定、MPLS則是結合了傳統路由技術與第二層標記交換技術的VPN技術，能提供更好的效能。

常見之 VPN協定技術與其應用範圍

- IPSec是新一代IP加密協定。
  - 也是 IPv6中的封包加密的標準。
- PPTP是基於PPP所設計的虛擬私有網路技術。
- L2TP結合了L2F與PPTP的優點而成爲新一代的第二層虛擬私有網路的通道協定。
- MPLS技術是一個可以在多種第二層協定上進行標籤交換的網路技術，不必改變現有的路由協定。
- SSL VPN由於方便成爲目前極受歡迎的VPN技術。

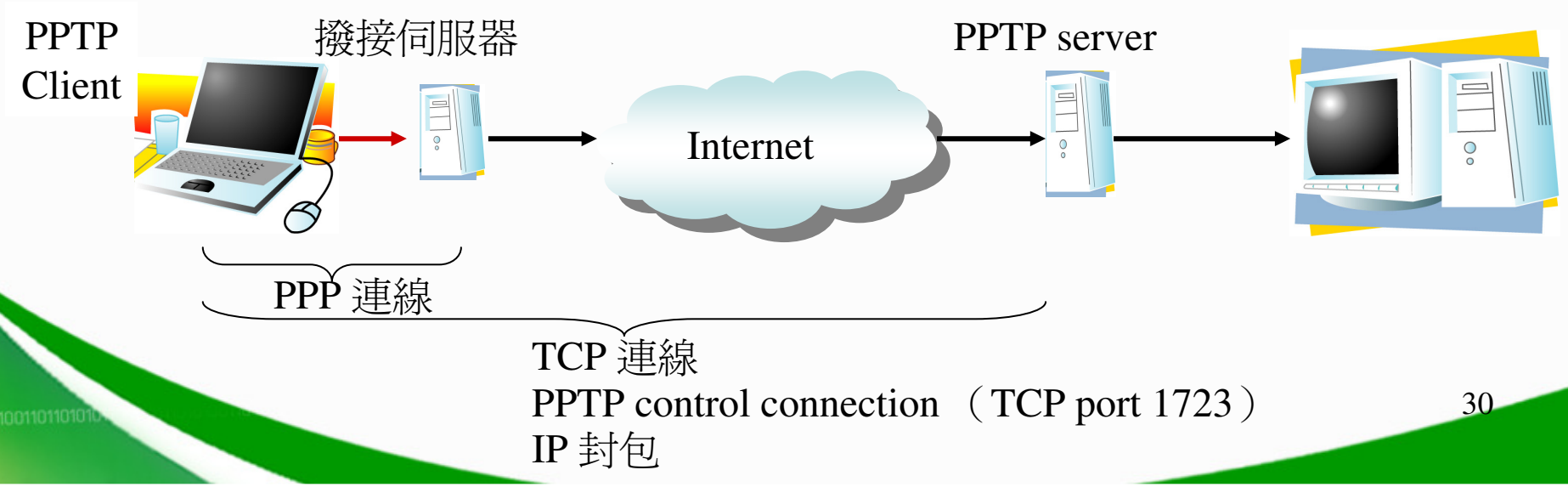
2-2 PPTP協定

Point-to Point Protocol（PPP）

- 最常見的撥接協定
- 運作在OSI第二層
- 可支援下列鑑別方式：
  - PAP、CHAP、MS-CHAPv2、RADIUS…
- 具備加密與壓縮能力
  - RC4、DES、3DES

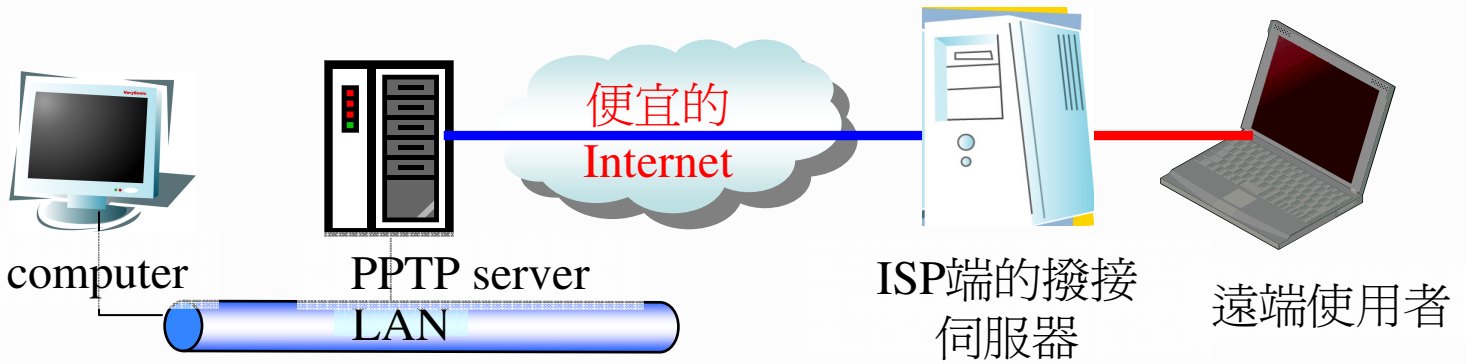
Point-to-Point Tunneling Protocol
點對點穿隧協定（PPTP）

- PPTP是由 Microsoft、3COM等提出經IETF通過，有 Microsoft 的全力支援，微軟作業系統內建 PPTP，因此使用率相當高。
- 是OSI第二層的穿隧協定。
- 資料先封裝在 PPP 框架中，然後再加上IP封裝。



遠端存取VPN如何減低成本

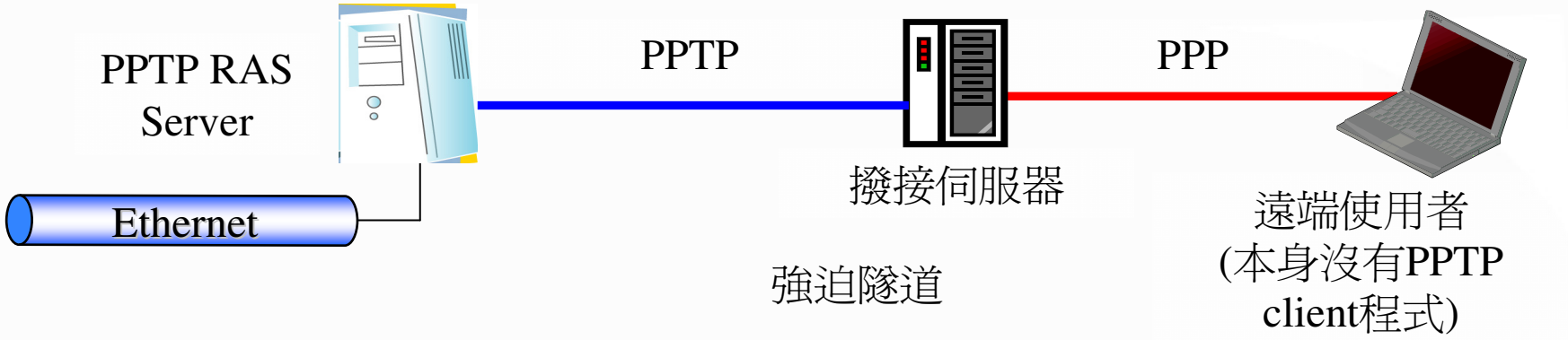
傳統遠端存取需撥接到企業提供的撥接伺服器

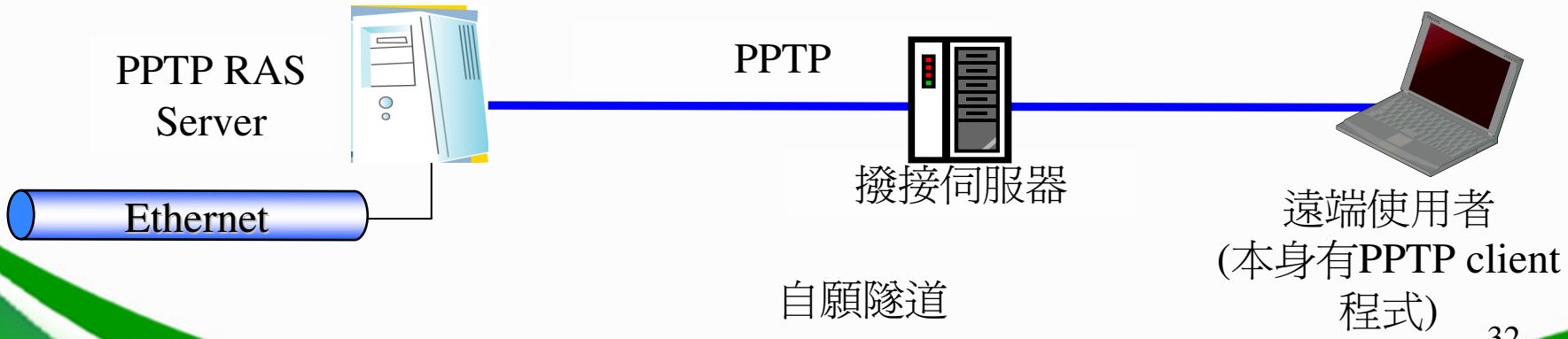


藉由L2TP或PPTP，利用近端ISP撥接伺服器，再建立通道至企業網路。

強迫隧道與自願隧道
(Compulsory tunnel and Voluntary tunnel)

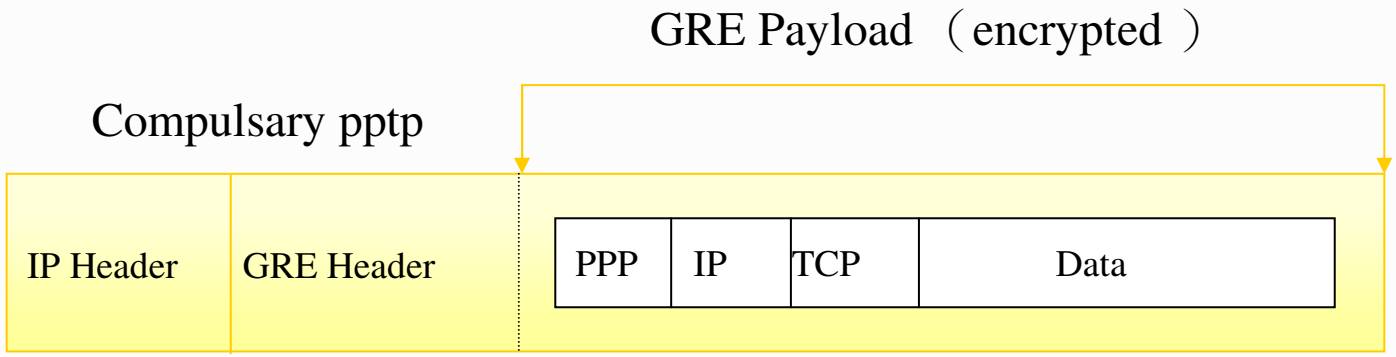
- PPTP有兩種使用架構



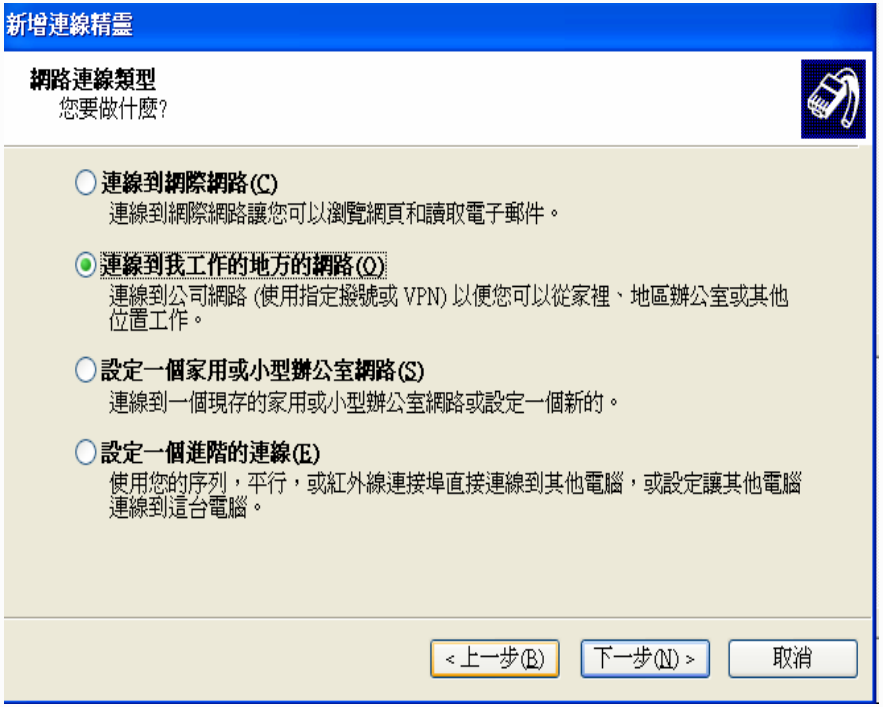


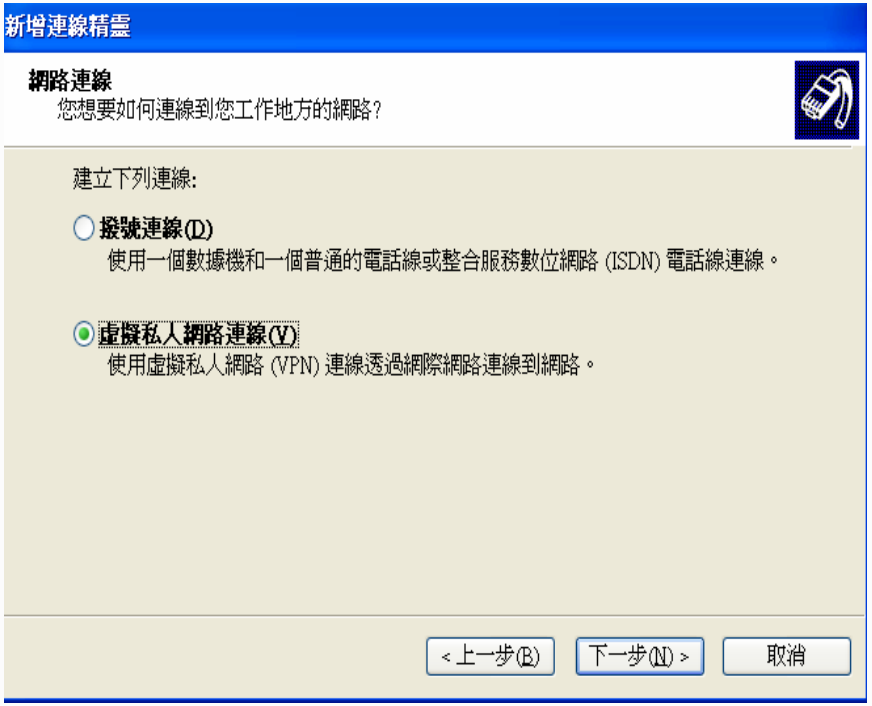
PPTP 封包格式

- Generic Routing Encapsulation（GRE）
  - 將一個Protocol封裝在另一個Protocol的規格
- 加密方式
  - Microsoft Point to Point Encryption（MPPE）



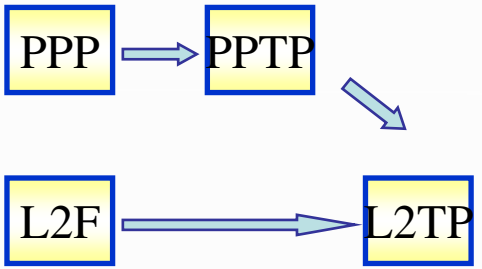
PPTP 用戶端設定方式





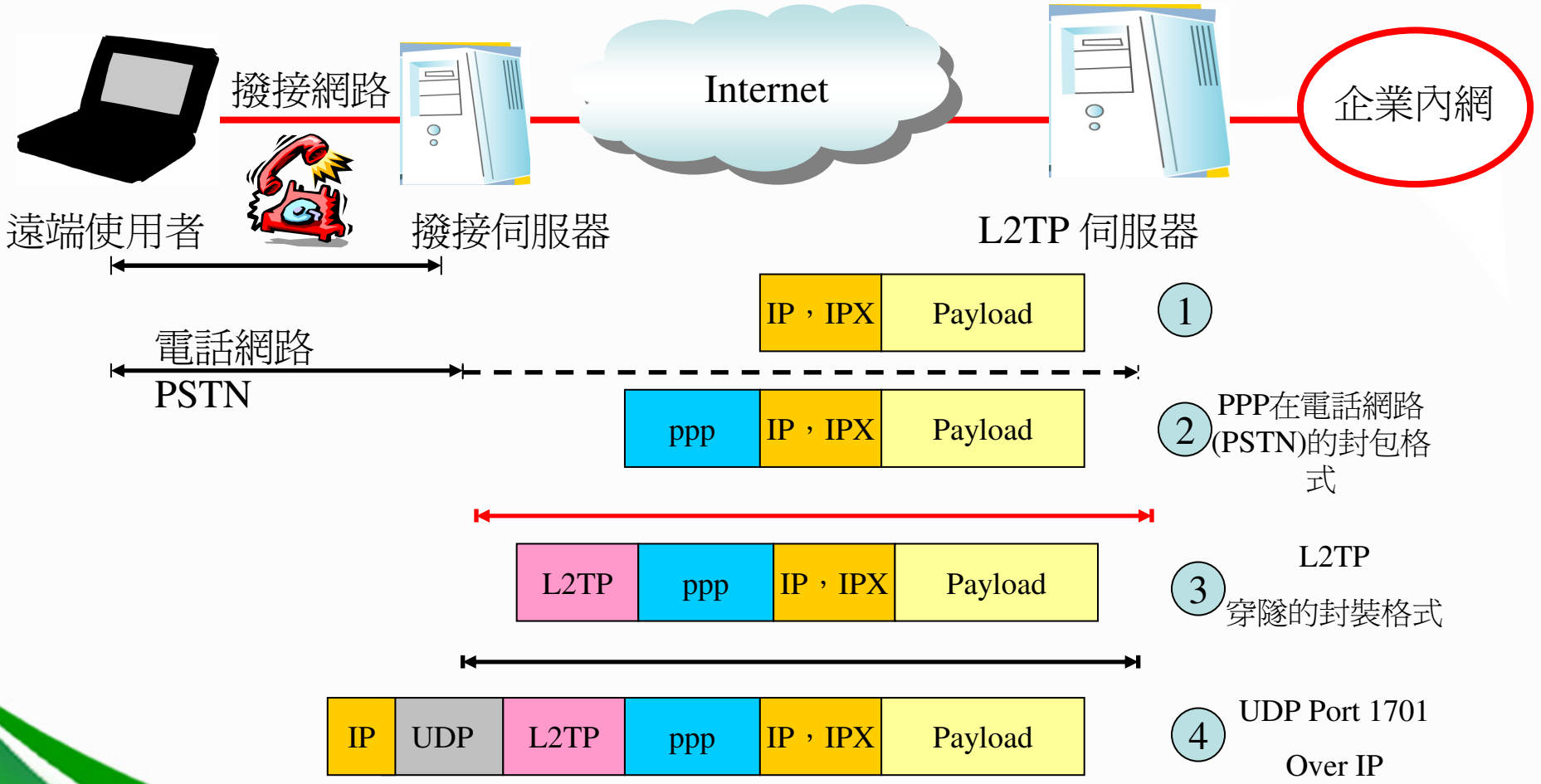
2-3 L2TP 協定

L2TP協定



- 封包檔頭比 PPTP 檔頭短。
- 一個隧道可以容納多個連線，可降低頻寬負擔。
- L2TP使用 IPSec 來替 TCP/IP 傳輸加密（所以是一種 L2 / L3 VPN）。
- 使用 UDP 來傳送 Control/Data 封包。

L2TP – 強迫隧道


撥接網路
Internet
企業內網
遠端使用者
撥接伺服器
L2TP 伺服器
電話網路
PSTN
IP，IPX
Payload
1
ppp
IP，IPX
Payload
2
PPP在電話網路(PSTN)的封包格式
L2TP
ppp
IP，IPX
Payload
3
L2TP穿隧的封裝格式
IP
UDP
L2TP
ppp
IP，IPX
Payload
4
UDP Port 1701 Over IP

2-4 IPSEC協定

IPSEC

- 保障IP網路上的傳輸安全性。
- 運作在OSI第三層（IP layer）。
- 提供多樣的設定組合安全連線。
- 具備金鑰管理功能（Key management）。
- 也是下一代 IP 協定（IPv6）的安全功能。

IPSEC 的模式

- AH模式（Authentication Header）
  - 只有確認封包的完整性與不可否認性的功能。

- ESP模式（Encapsulating Security Payload）
  - 定義加密的標準與封包的完整性，擁有驗證和加密的功能。

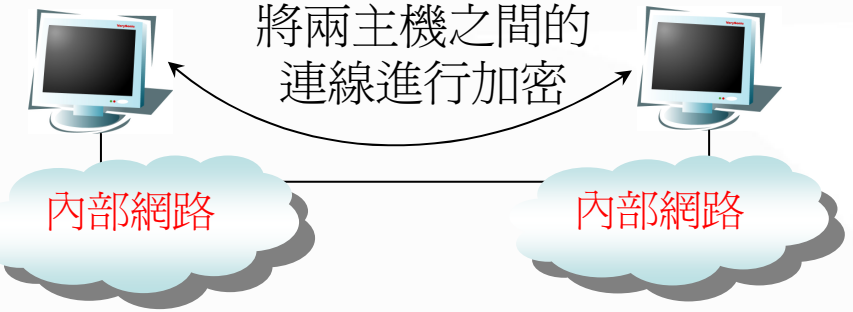
套用 ESP之前

套用 Transport mode ESP之後

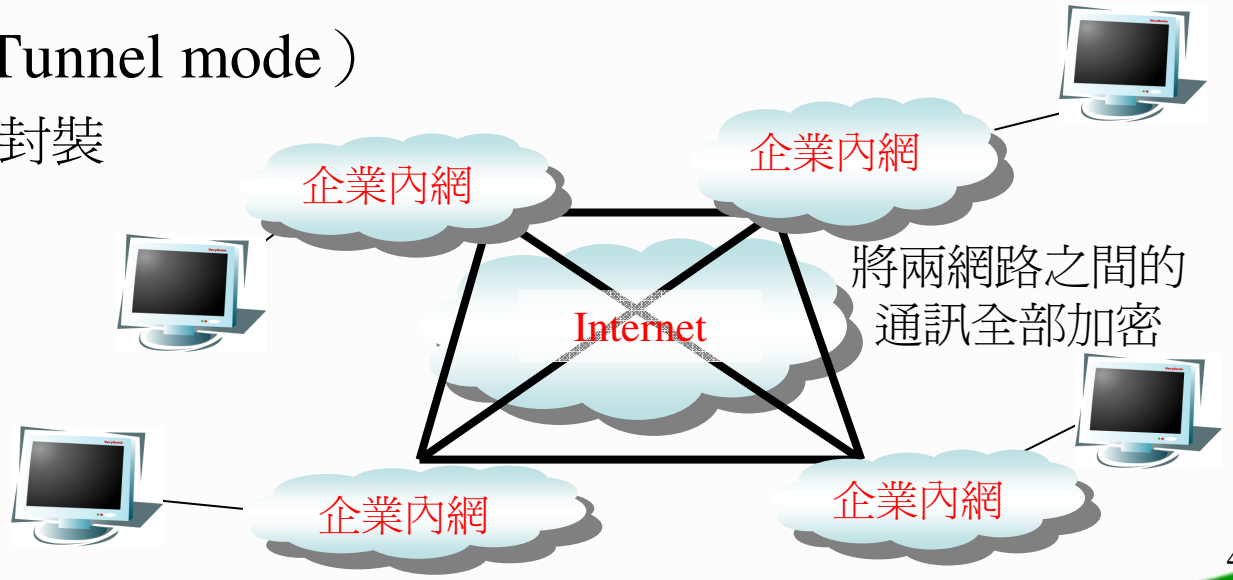
傳輸模式與隧道模式 (Transport mode / Tunnel mode)

支援兩種封裝模式

- 傳輸模式（Transport mode）
  - 將封包加上檢查標頭



- 隧道模式（Tunnel mode）
  - 將整個封包封裝



IPSEC 的運作原理

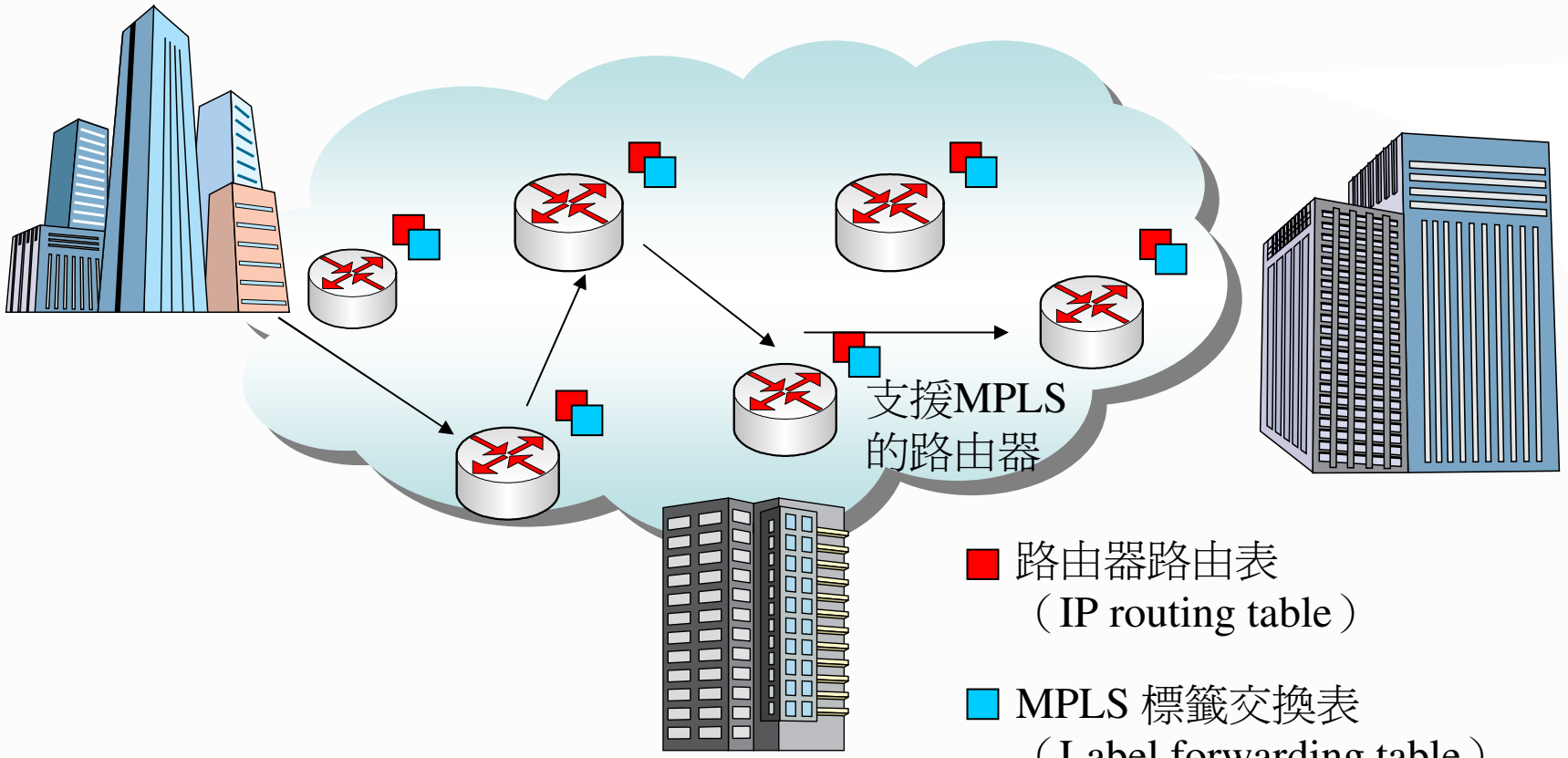
- Security Associations（SA）
  - 一個連線中所含的一組安全服務。所以在建立了一個IP連線時，任何的AH或是ESP功能都定義爲一個獨立的SA。
  - SA包含下列內容
    - 安全參數索引（SPI,Security Parameter Index）、目標IP位址、 安全協定等…
- IPSEC的金鑰管理機制
  - Internet Key Exchange（IKE）
    - ISAKMP+OAKLEY
  - ISAKMP只是平台架構（ framework）
  - OAKLEY是ISA KMP所使用的金鑰交換技術
  - OAKLEY改良了一些Diffie-Hellman所沒有的安全機制

2-5 MPLS 技術

MPLS多重協定標籤交換技術

- MPLS多重協定標籤交換技術（MultiProtocol Label Switching）爲新一代確保網路通訊品質的通訊協定。
  - MPLS 結合了 IP、ATM 與 Frame Relay 等網路架構的優點，可運作在這些網路架構之上。
  - 能依需求提供服務品質保證（QoS），解決原本IP VPN無法有效提供 QoS 保證的缺點。
  - 目前應用於 IP 網路之上，如 IP VPN（Virtual Private Network）網路上加上 MPLS 的功能爲目前當紅之應用。

MPLS 多重協定標籤交換技術運作原理



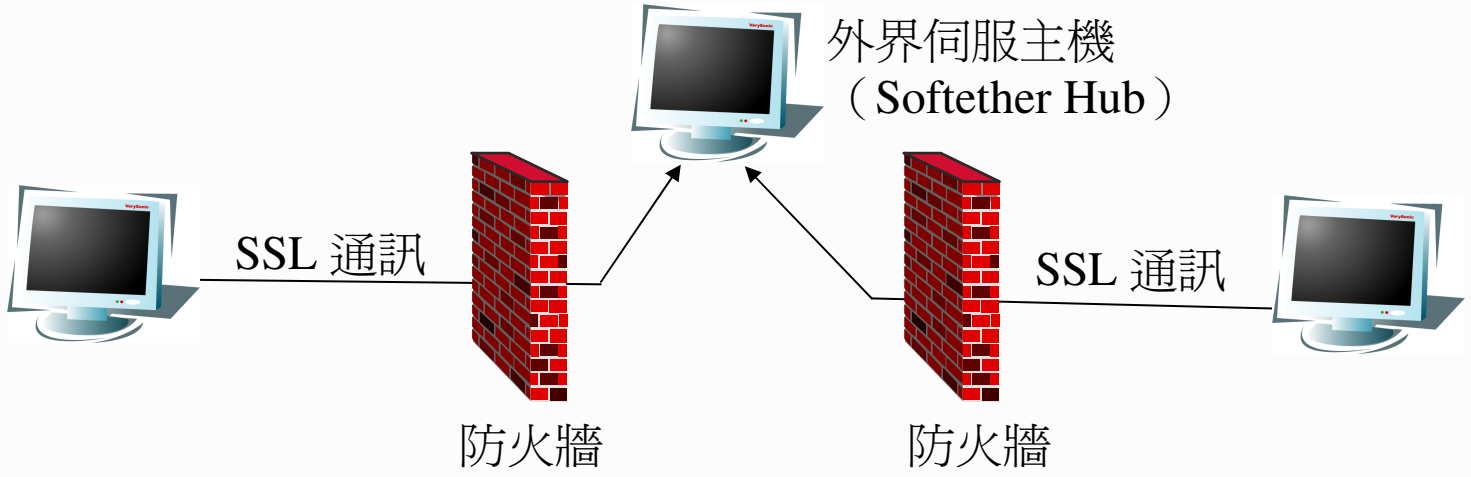
2-6 SSL VPN 技術

SSL VPN技術

- SSL爲Secure Socket Layer的簡稱。
- 適用於遠端存取型VPN 。
- 由於SSL VPN設定比IPSEC、PPTP來得簡易，因此成爲近幾年當紅的 VPN 存取技術。
- 簡易的 SSL VPN，用戶端不需安裝軟體，利用瀏覽器介面，便可連線至企業內網。
- 缺點：由於基於 SSL，並非所有 IP層的應用程式都可使用。

另一種 SSL VPN – SoftEther軟體

- 日本大學生所研發，可將主機通訊藉由SSL對外連線。
  - 藉由 SSL 通訊，將兩部或多部主機連接。彷彿位於同一區域網路（虛擬 Hub）



電腦A、B、C彼此彷彿就像內網主機一般

2-7 各項 VPN 協定技術比較

各項VPN協定技術比較表

	運作階層	優 點	缺 點
PPTP	OSI 第 2層	適用遠端存取，由MS推廣，Windows系統內建PPTP client	標頭檔過大，每個隧道僅能支援一個連線
L2TP	OSI 第 2和3 層	適用遠端存取， IP部分使用IPSEC加密，由L2F與PPTP改進而來，每個隧道能支援多個連線	需要設定使用者端軟體
IPSEC	OSI 第 3 層	擁有完整規格，爲下一代網路IPv6之加密標準	僅運作在OSI第3層(IP層)
MPLS	OSI 第 2和3 層	基於IP-based的交換技術,爲目前最常見之service provider VPN技術，傳輸速度快	需經由ISP業者提供服務，無加密措施
SSL VPN	Secure Socket Layer	使用瀏覽器，設定最簡便	由於建構於SSL，並不是所有程式都支援

第三章 VPN 的應用與風險簡述

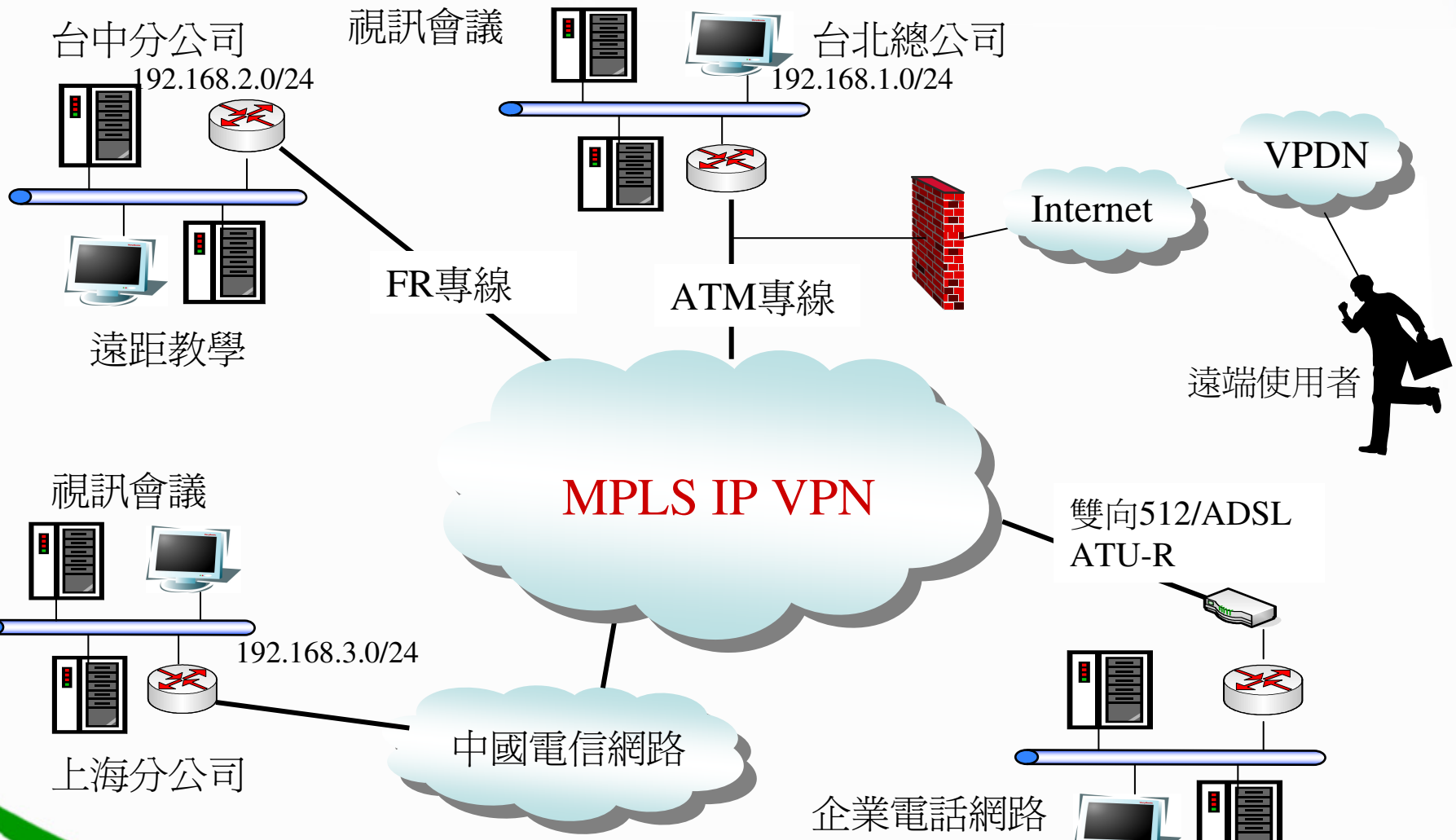
- 3-1 VPN 的應用與風險
- 3-2 GSN VPN 介紹

3-1 VPN 的應用與風險

VPN 的應用

- 建構企業、政府機關網路。
- 應用於企業專屬電話網路、視訊會議。
- 遠距教學、遠距醫療。

VPN 的應用實例


台中分公司
192.168.2.0/24
視訊會議
台北總公司
192.168.1.0/24
VPDN
Internet
FR專線
ATM專線
遠距教學
遠端使用者
MPLS IP VPN
視訊會議
雙向512/ADSL
ATU-R
192.168.3.0/24
中國電信網路
企業電話網路
上海分公司
192.168.4.0/24
高雄分公司

VPN的風險說明

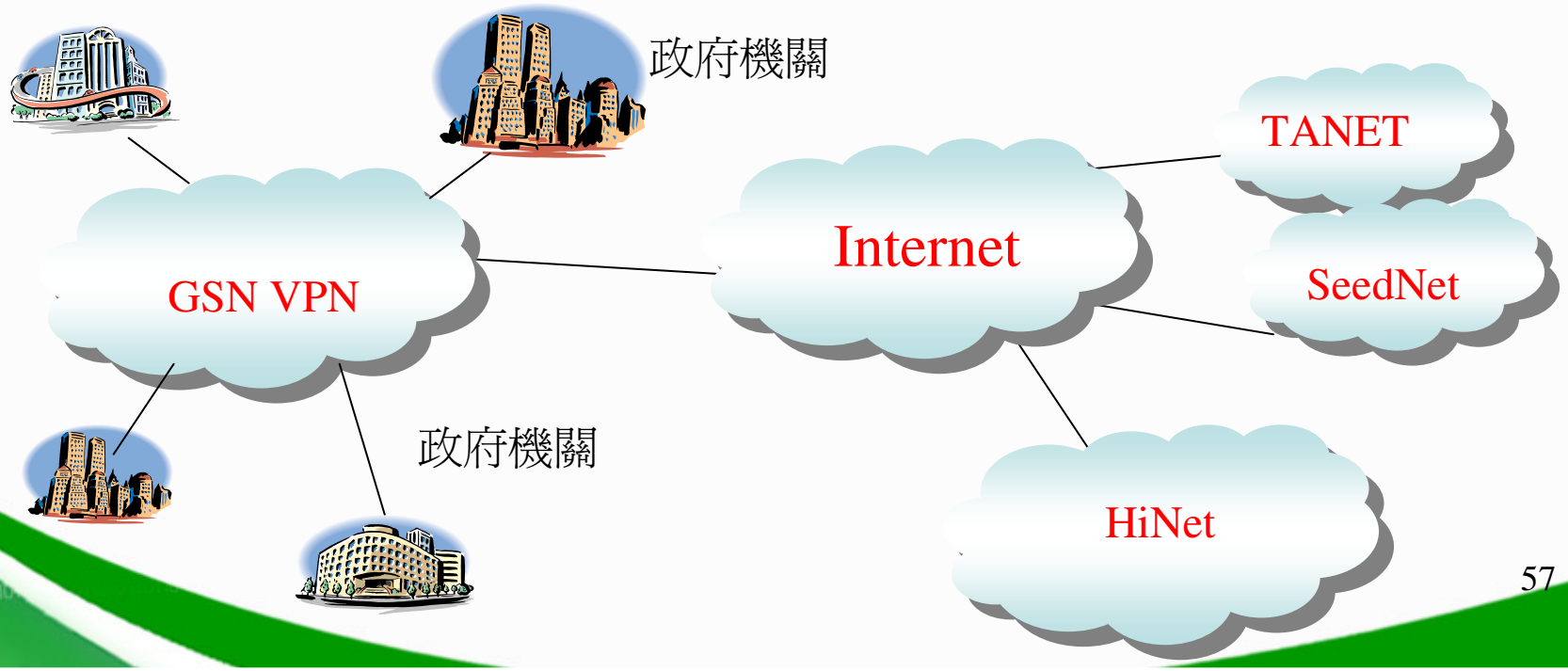
- VPN並非完全安全的封閉網路
  - 一旦網路蠕蟲進入VPN內部網路，仍可在內部造成危害。

    例如：筆記型電腦夾帶的病毒或蠕蟲
  - 由於VPN仍會對外連接Internet，現在常見的Email木馬，藉由使用者收信行爲進入內網，亦成爲VPN內網最大威脅之一。
- VPN所開啓的遠端撥接伺服器，需進行定期稽核與管理，避免駭客盜取帳號後，藉此取得進入企業內網的能力。
- 目前許多用戶藉由ADSL接取方式連上企業VPN，一旦連線帳號被盜用，亦可讓駭客進入企業內網。

3-2 GSN VPN介紹

GSN VPN簡介

- GSN（Government Service Network，政府網際服務網）
- 爲了推動電子化政府，由行政院研考會推動，爲國內各政府機關建構安全的網路環境。

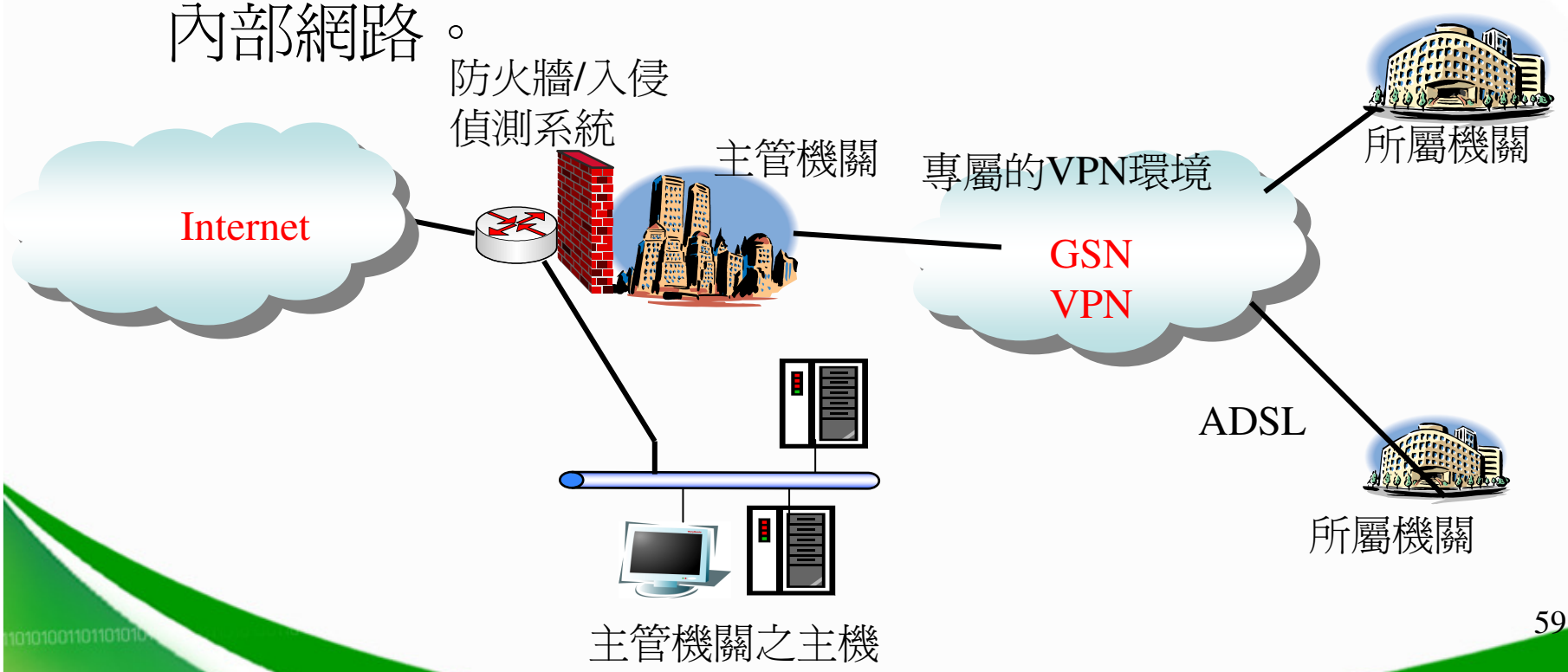


GSN VPN 特色

- 頻寬保證
- 安全管理
- 可靠度
- 分布廣、時效快
- 彈性大
- 提供網管功能

GSN 應用實例

- 某政府機構下共有兩個所屬單位，分別藉由ADSL連上GSN網路，並統一由該政府機關連接上Internet，透過防火牆與入侵偵測系統來保護整個內部網路。



第四章 結論

結論

- 虛擬私有網路利用穿隧、加解密等安全技術，在公眾網路上，建構出安全的虛擬的私有網路。
- 爲了解決TCP/IP傳輸安全問題，IPsec成爲VPN解決方案之一，也是下一代IPv6網路的安全標準。
- MPLS VPN是基於MPLS網路的VPN架構，在2001年IETF公佈MPLS標準之後，公認成下一代網路基礎協定。

結論（續）

- PPTP是針對移動式使用者需求，而由於微軟在作業系統內建PPTP，使得PPTP成爲遠端存取型VPN最常用的通訊協定。
- 目前Web應用程式已成爲趨勢，加上移動員工與在家辦公人員的增加，因此SSL VPN成爲另一股與IPSEC/MPLS VPN市場互補的發展力量。

課程結束