Outline

- Introduction
- IP Address & MAC Address
- TCP / UDP / ICMP
- IP Gateway, Network Mask, TTL
- Routing Protocol
- Network Address Translation (NAT)
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP) / Asymmetric Digital Subscriber Line (ADSL)
- HyperText Transfer Protocol (HTTP)
- **Virtual Private Network (VPN)**
- Firewall
- Wireless Networks

Virtual Private Network(VPN)，虛擬私有網路

- 使用公眾線路建立的安全通訊連結網路，
  EX:在任何連接**Internet**的電腦上，可使用支援**VPN**的通訊協定來建立一個其他人無法介入竊聽的連結；
- **VPN**也可說是一種讓公共網路(如**Internet**)變成像是內部專線網路的，來提供使用者有如內部網路的安全性與優先性等功能。
- 而透過公用網路來建立與遠端使用者、分公司及合夥人建立專屬的網路連結；其原理是在分封交換網路中透過特殊應用軟體，將用戶具相關性的電路設定成專用網路，供其網路內各點相互通信

❖ VPN可以分成三大項目

- 遠端存取(Remote Access)
  連結移動用戶(Mobile User)及小型的分公司，透過電話撥接上網來存取企業網路資源。
- Intranets VPN
  是利用Internet來將固定地點的總公司及分公司加以連結，成爲一個企業總體網路。
- Extranets VPN
  將Intranet VPN的連結再擴展到企業的經營夥伴，如供應商及客戶，以達到協力廠商彼此資訊共享的目的。

爲何要用VPN？

❖ 相較於傳統的專線式網路連結，VPN架構的優點：

- 成本較低。
  VPN的架設在設備的使用量及廣域網路的頻寬使用上均較專線式的架構節省，故能使企業網路的總成本(Total Cost of Ownership) 降低。根據分析，在LAN-to-LAN的連結上，VPN將較專線式的架構成本節省20% ~ 40%左右；而就遠端存取(Remote Access)而言，VPN更能比直接撥接至企業內部網路節省60% ~ 80%的成本。
- 網路架構彈性較大。
  VPN較專線式的架構來的有彈性，當有必要將網路擴充或是變更網路架構時，VPN可以輕易的達成；相對的，傳統的專線式架構便需大費周章了。
- 管理方便。
  較少的網路設備及實體線路，使網路的管理較爲輕鬆；不論分公司或是遠端存取用戶再多，均只需透過Internet的路徑進入企業網路。

構成VPN的要件

- **VPN**網路的形成，必定要有幾個重要的要素及條件，以確保資料能被安全、及時的傳輸於公眾網路之上。這些要件分別是：
  - VPN平台的擴展性(Platform Scalability)
  - 安全(Security)
  - VPN服務

VPN平台的擴展性(Platform Scalability)

- VPN的平台需要具備完整的擴展性，大至企業總部的設備，小至各分公司，甚至個人撥接用戶，均可被包含於整體的VPN架構中。同時，VPN的平台亦需保留有對未來廣域網路頻寬擴充及連結架構更新的彈性。

安全(Security)

- 過去企業的網路架構，多以封閉式的專線連結爲主；其主要考量即是在於資料傳輸的”安全性”。若在安全性不能被保障的狀況下，一旦企業重要資料被駭客或有心人士所竊取，將對企業造成難以彌補的傷害及損失。這樣的危機考量，絕對是較網路建置成本、便利性等因素來的更爲重要，且不可替代。所以在**VPN**架構中的各項安全機制，諸如通道**(Tunneling)**、加密**(Encryption)**、認證**(Authentication)**、防火牆**(Firewall)**及駭客偵防系統**(Intrusion Detection)**等技術，便成爲**VPN**技術中最爲重要的一環。
- **VPN**的建置中，必需透過上述的各項網路安全技術，確保資料在公眾網路中傳輸時不致於被竊取，或是縱使被竊取了，對方亦無法讀取封包內所傳送的資料。如此才可讓**VPN**的架構，取代傳統的專線式網路連結，而仍然讓企業的資料傳輸擁有相同的”安全性”保障。

VPN服務

- 頻寬的管理及服務品質(Quality of Service，QoS)服務的提供，來確保資料透過公眾網路傳輸時的及時性，避免網路的阻塞，並提供封包資料的等級分類及傳送。

VPN的產品種類

- 市面上**VPN**產品相當多，不過可以區分成三大種類：
  - 硬體式的VPN系統
  - 軟體式的VPN產品
  - 與防火牆相結合的VPN系統

- 硬體式的**VPN**系統

  最常見的硬體式的**VPN**設備便是**VPN**加密的路由器**(VPN Router)**。因爲這些設備將加解密的鑰匙儲存於記憶體中，故較不易被損壞，同時加解密的速度亦較快；尤其是專線頻寬較高之企業，硬體式的設備應是較佳的選擇。此外，若再搭配個人用戶使用的**VPN**軟體**(VPN Client Software)**，則其功能亦與軟體式的**VPN**產品相近。

- 軟體式的**VPN**產品

  軟體式的**VPN**產品乃是架設於伺服器及作業平台之上，可以提供較爲彈性的功能，例如依據目的地位址或通訊協定來建立**VPN**通道。相對的，硬體式的**VPN**系統則多數依據位址目的地來建立**VPN**通道，將傳輸的所有通訊協定均加密。

  然而，軟體式的**VPN**產品通常較難以管理；需要對作業系統、**VPN**軟體及相關之網路安全機制均有相當程度的了解，才能真正管理好**VPN**系統。同時，有些**VPN**軟體亦需要對路由路徑表**(Routing Table)**及網路**IP**位址規劃**(Network Address Scheme)**加以修改。

- 與防火牆相結合的VPN系統

  此系統自然承襲了防火牆安全功能的優點，使進出的交通均能受到較佳的限制及保護，以及強化的認證功能。一般而言，相當多的VPN廠商並沒有提供對於其作業系統的安全保護。若是採用硬體式且具有VPN功能的防火牆設備，則本身便已對其運作的作業系統做了補強作用，事先將所有不必要及有危險的服務(Service)均加以去除，以確保此VPN設備不會被駭客所入侵，而導致整體VPN系統功能無法運作。

  同時擁有VPN及防火牆功能的設備，對於網路的安全建構有相當大的好處，只需一台機器便可擁有兩項不可或缺的功能，建置成本明顯降低，且管理的負擔亦較輕。

VPN的注意事項(1/4)

1. 企業對於VPN的建構及應用上，並不應該將原有的廣域網路架構完全替換掉，而是要在既有的廣域網路架構上加上VPN的功能，改變網路的邏輯架構，進而得到VPN節省成本、具彈性且易於管理的優點。若是完全引進新的VPN設備而不利用現有之廣域網路設備來做爲VPN之節點，則勢必使建置之成本倍增，且增加網路架構之複雜性；反之，若能使用現有的路由器(Router)、防火牆(Firewall)等設備，使之成爲VPN的節點，則可大幅降低VPN的建置成本，並且易於管理。

VPN的注意事項(2/4)

2. VPN的資料均需在加密之後，才由公眾網路傳送至接收端，再由接收端設備加以解密。故每一個封包在整個傳輸過程中均需被加、解密一次，而加密、解密均是相當消耗VPN設備運算能力的工作。因此，VPN設備的加解密速度表現，快者可達100Mega，慢者則只有幾Mega的速度，亦是在架設VPN時必需要謹慎考量的因素。如上節所述，硬體式的VPN產品在運作效能上會比軟體VPN產品有較佳的表現。故在使用量較大、對加解密及傳輸速度在意的用戶，應以硬體式的VPN產品，如VPN路由器及擁有VPN功能之硬體防火牆爲較佳之考量。

VPN的注意事項(3/4)

3. 考量VPN產品的連結相容性，未來的VPN產品均會以IETE所公佈的IPSec協定爲標準，來作爲彼此資料加解密、傳輸的依據。然而到目前爲止，在實際的應用上，不同廠牌的VPN產品仍常會有連結上無法完全相容的問題。故就現實面而言，仍應以同一廠牌之VPN產品做爲企業體VPN 建置的設備，所需面臨的困難最少。也因爲如此，選擇足夠規模、能夠提供完整的VPN解決方案的廠商，亦成立VPN建構中重要的課題。而所謂的VPN完整解決方案極是包括遠端撥接(Remote Access，Client-to-LAN VPN)、Intranet VPN & Extranet VPN (LAN-to-LAN VPN)等架構，以及擴充性佳、完整網路安全功能、以及VPN服務(QoS Service)等項目。

VPN的注意事項(4/4)

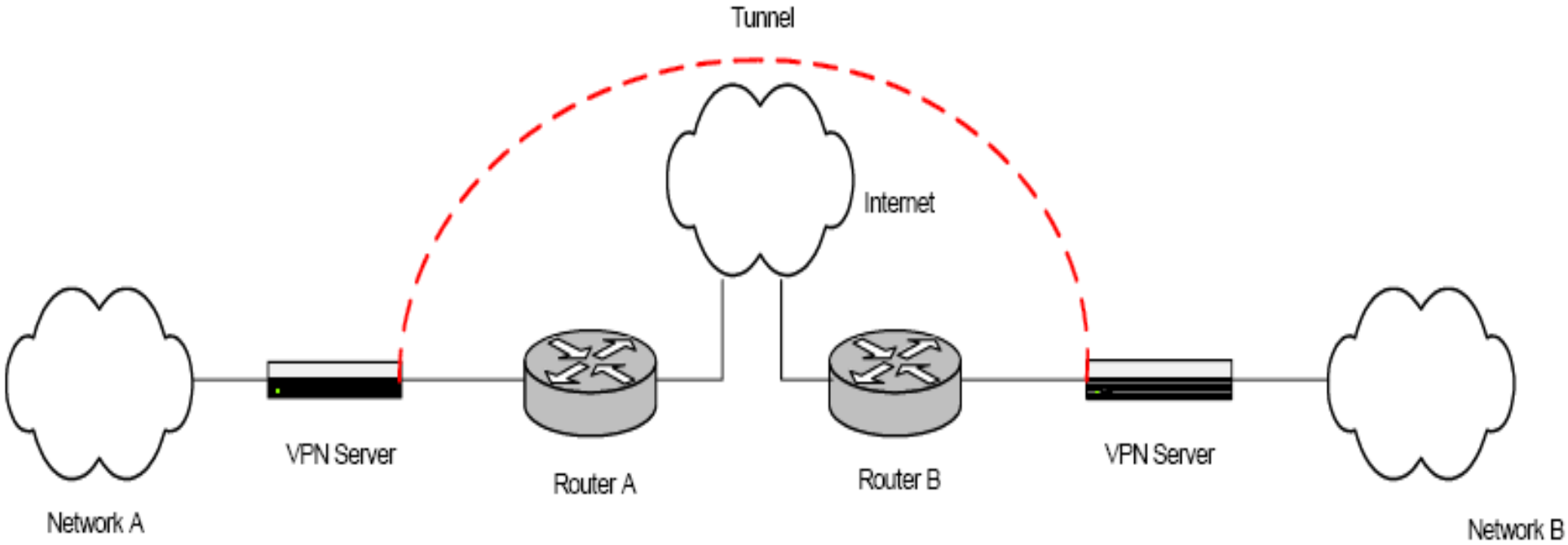
4. 在VPN架構安全考量的使用者認證部份，若能以集中式的管理方式(Centralized Management)來運作，必能減少網路管理的負擔。網路上需要有認證機制的設備，除了VPN產品之外，亦有防火牆及遠端撥接伺服器(Remote Access Server)等設備。若所有這些設備均能透過單一的安全認證伺服器來做認證的工作，則無論未來網路如何擴充，永遠只需一套認證伺服器即可滿足需求。

VPN –Virtual Private Network

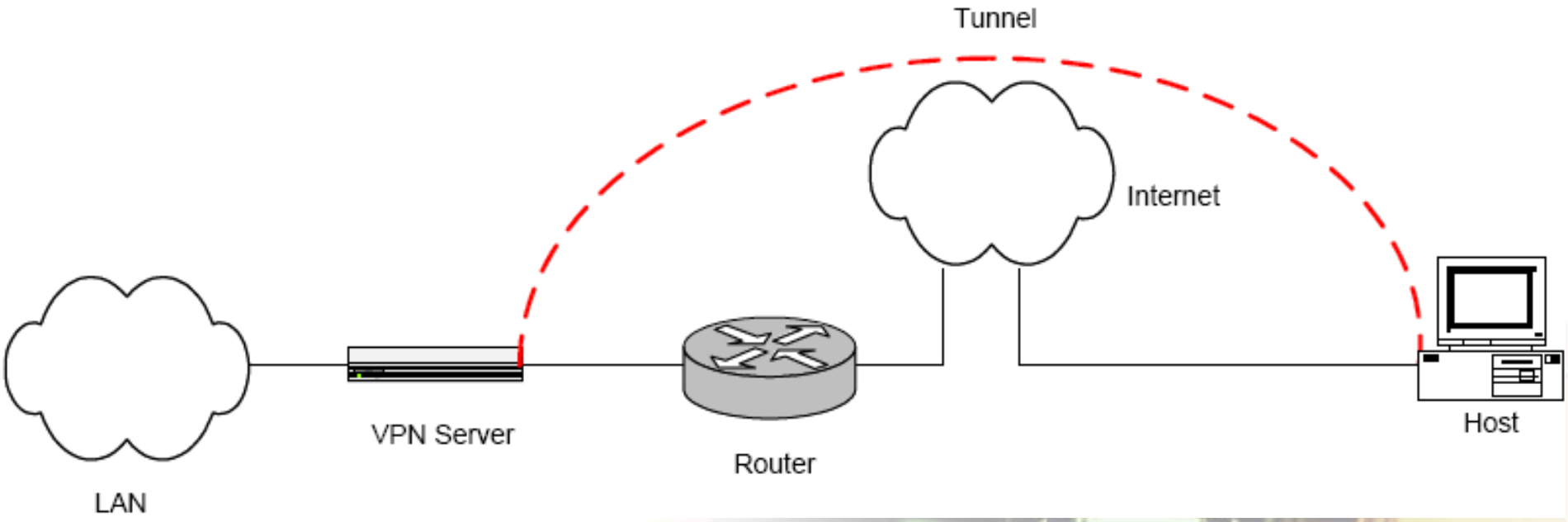
- **Virtual Private Network :**
  在現有的公眾通訊網路的架構之下，利用Tunnel和安全的機制，讓資料的傳輸能保持隱私的Private Network。
  - **Trusted VPNs:**
    指的是**VPN** 客戶相信**VPN**網路提供者能夠使用最好的機制以確保**VPN** 網路不被監聽。
  - **Secure VPNs:**
    將傳送的資料加密**(Encryption)**的**VPN**。
  - **Hybrid VPN :**
    Secure VPN 可以是**Trusted VPN** 的一部份，這種**VPN** 稱爲**Hybrid VPN**。

三種VPN實做方式(1)

- **1. LAN to LAN**：兩個私人網路之間的連線。

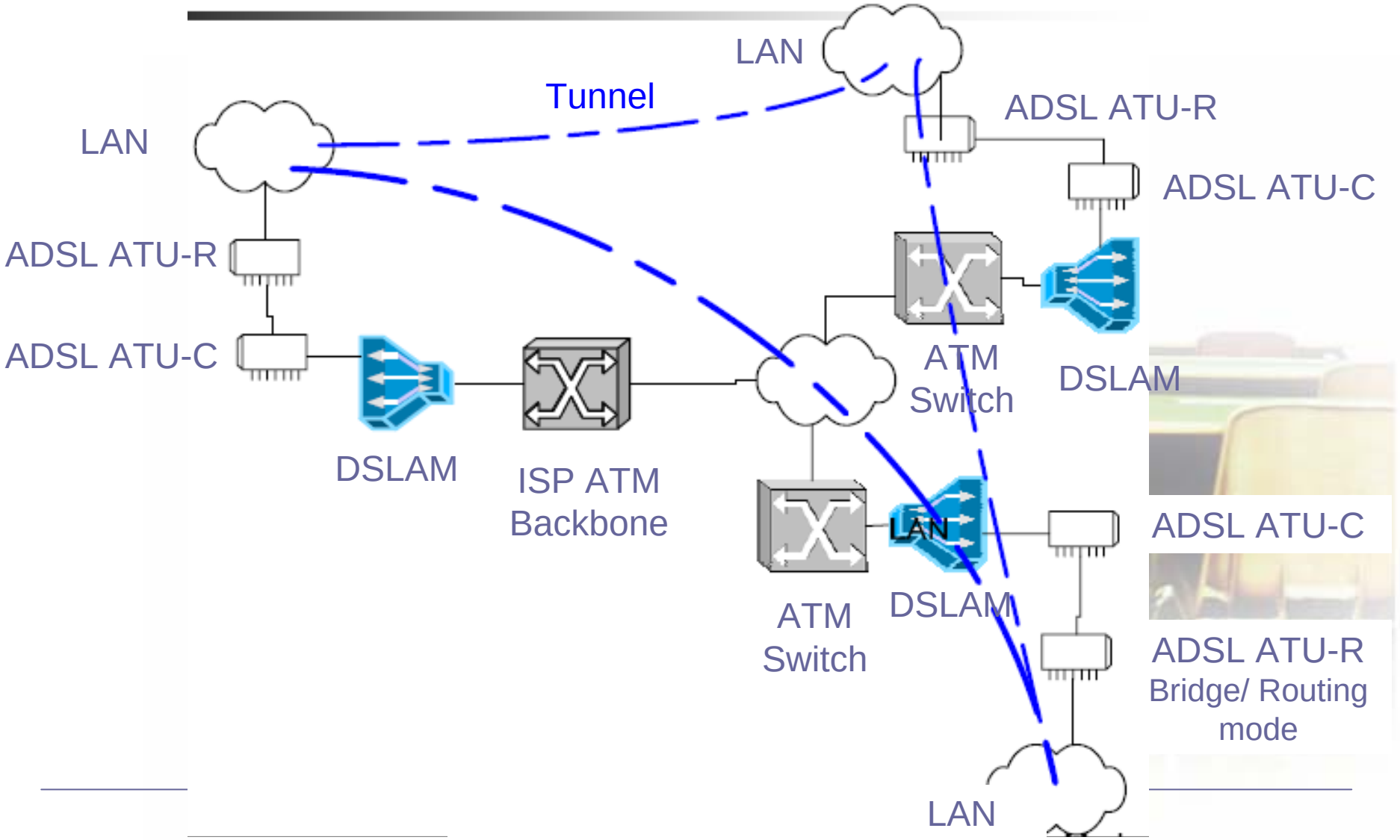


❖ **2. Host to LAN**：由外部網路的工作站，連線至私人網路。



三種VPN實做方式(3)

❖ 3. 以ISP骨幹網路做爲VPN媒介



Tunneling

- **Tunneling:**
  在兩台VPN 主機間建立一個專有的通道，作類似Circuit Switching 中Channel 的觀念，但實際上還是在原有的網路架構之下運作。

VPN應用之相關協定

Generic Routing Encapsulation (GRE)

- 將network A經由GRE封裝，傳送至network B
- 屬於Layer 3的協定
- GRE是用在VPN中Tunnel的技術

Point to Point Tunneling Protocol (PPTP)

- PPTP是一個常用在VPN中的一個協定，藉由GRE header，將資料從IP packet換成PPP packet
- 加入連線認證機制，採用client-server模式，稱爲Enhance GRE

IP Security Protocol (IPSec)

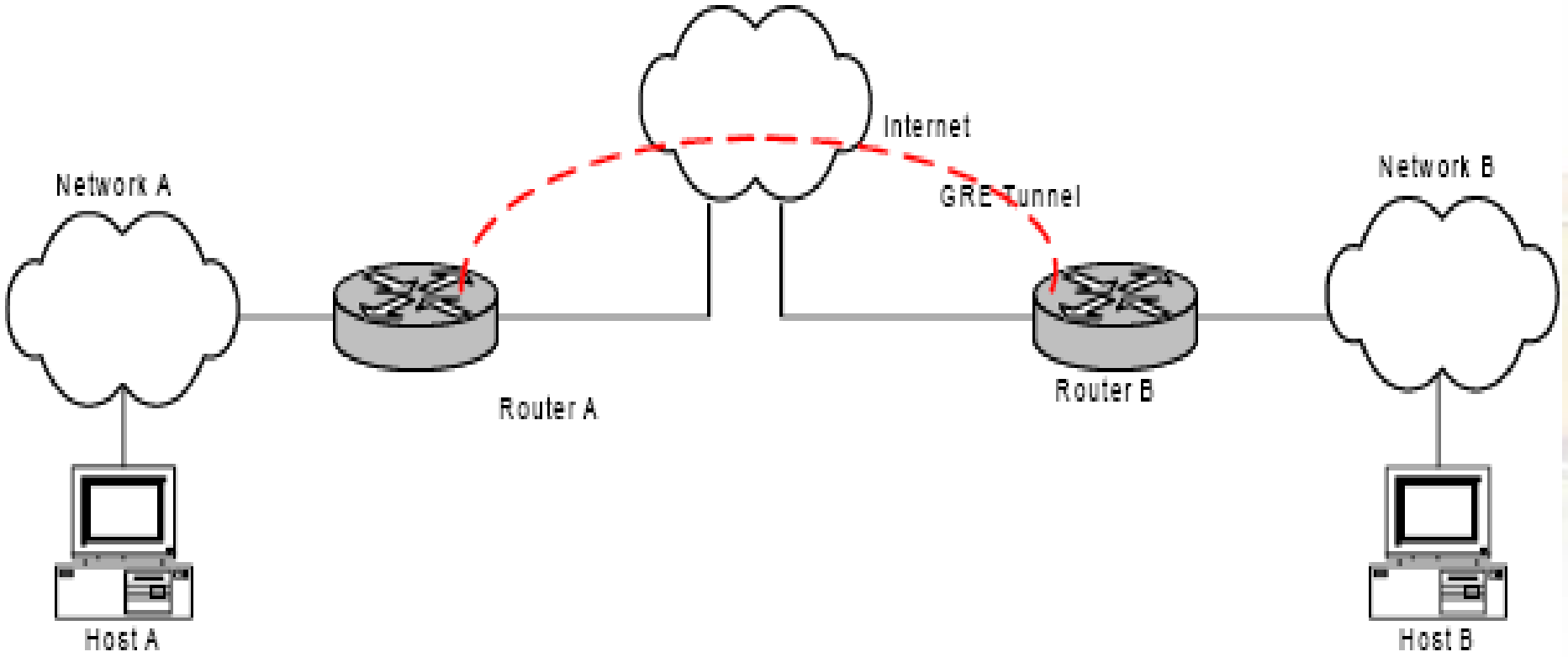
- 屬於IP Protocol的延伸，它提供了一個使用密碼將欲傳送的Packet加密的一種服務，使任何的IP protocol能夠使用一個”加密”的Tunnel

Generic Routing Encapsulation (GRE) 1

- GRE傳遞的實例
  1. 在Network A的Host A 欲傳送資料給在於Network B的Host B
  2. Host A經由Network A的網路傳送Packet給Router A ，Router A判斷Packet的目的地，以決定要如何傳送Packet。
  3. Router A將Packet以GRE封裝送到Internet上。
  4. Router B收到這個GRE Packet並且判斷出是以GRE方式封裝。

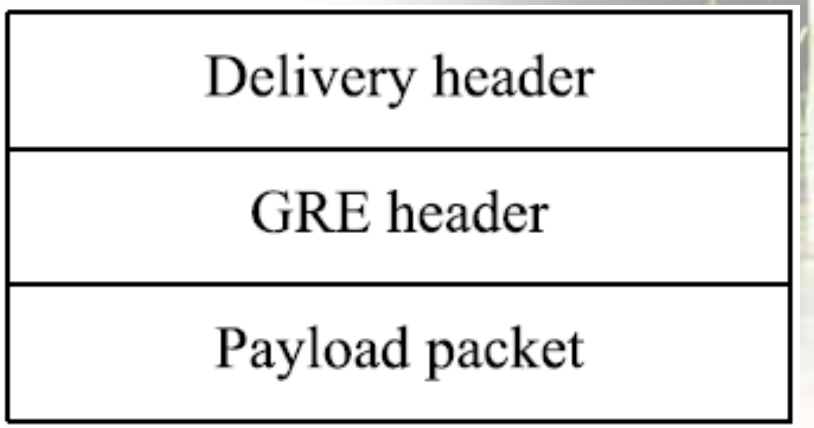
Generic Routing Encapsulation (GRE) 1

5. Router B解封裝(Unwarp)
6. Router B將封裝後的Packet經由Network B送給Host B。
7. Host B收到這個Packet。



Generic Routing Encapsulation (2)

- 完整的**GRE** 封裝:
  當系統中有一個packet要被封裝及繞送，稱爲“Payload Packet”。這個payload packet首先會被GRE Header封裝，在GRE Header的內容中可能包含了路由資訊。之後必須再封裝一層其他的Protocol才能真正的送到Internet上，我們將這層protocol稱之爲”Delivery Protocol”。



Generic Routing Encapsulation (3)

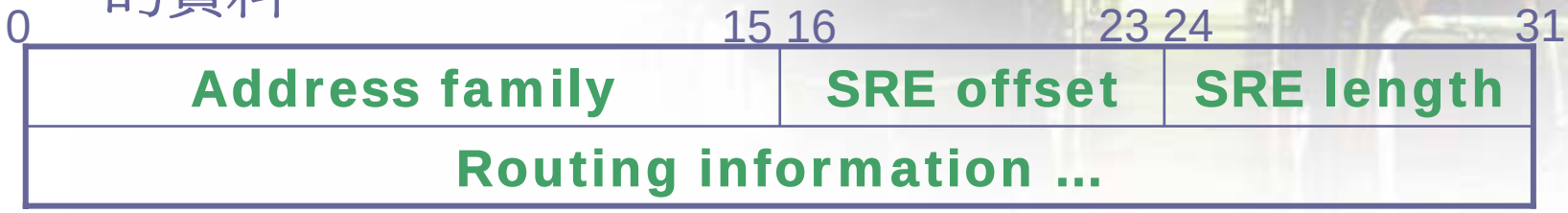
❖GRE Header定義

0	1	2	3	4	5-7	8-12	13-15	16-31
C	R	K	S	S	Recur	Flags	Ver	Protocol type
Checksum (optional)								Offset (optional)
Key (optional)								
Sequence number (optional)								
Routing (optional)								

C	(Bit 0) Checksum Present. Set to zero (0)
R	(Bit 1) Routing Present. Set to zero (0)
K	(Bit 2) Key Present. Set to one (1)
S	(Bit 3) Sequence Number Present. Set to one (1) if a payload (data) packet is present. Set to zero (0) if payload is not present (GRE packet is an Acknowledgment only).
s	(Bit 4) Strict source route present. Set to zero (0)
Recur	(Bits 5-7) Recursion control. Set to zero (0)
Flag	(Bit 8) Acknowledgment sequence number present. Set to one (1) if packet contains Acknowledgment Number to be used for acknowledging previously transmitted data. (Bits 9-12) Must be set to zero (0)

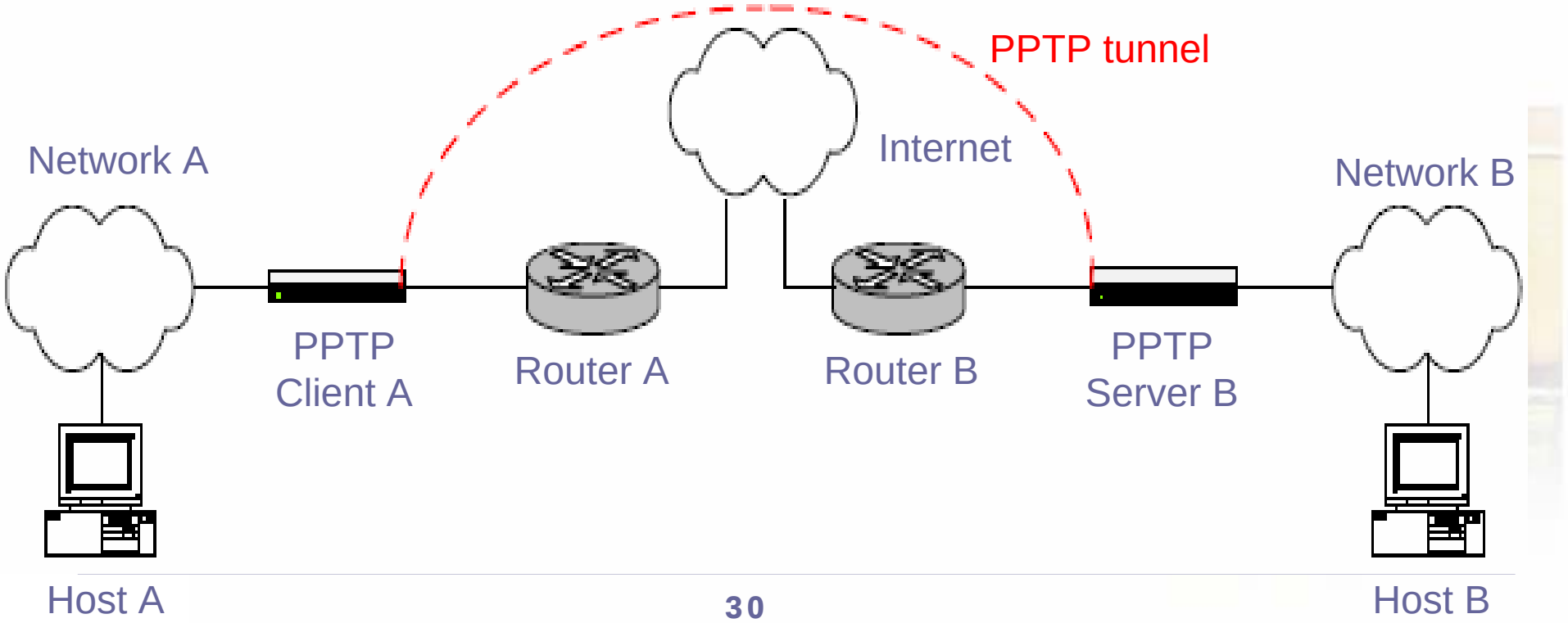
Ver	(Bits 13-15) Must contain 0
Protocol Type	Set to hex 880B (for PPP)
Checksum	Checksum with IP, GRE header and payload packet
Offset	Checksum or routing present is 1
Key (HW) Payload Length	(High 2 octets of Key) Size of the payload, not including the GRE header.
Key (LW) Call ID	(Low 2 octets) Contains the Peer's Call ID for the session to which this packet belongs.
Sequence Number	Contains the sequence number of the payload. Present if S bit (Bit 3) is one (1)
Routing	Source routing entries (SRE)

- **Routing (Variable) :**由一串的**Source Route Entries(SREs)**組成的。**SREs**的形式
  - **Address Family (2 Octets) :**包含了兩組八位元的**Routing Information Field**的語法和語義。
  - **SRE Offset (1 Octets) :** 含有來源處資訊的八位元無號整數。
  - **SRE Length (1 Octets) :** 含有**SRE**八位元組的數字，若**SRE Length**爲**0**，則此**SRE**乃爲**Routing Field**中的最後一組**SRE**。
  - **Routing Information (Variable) :** 擁有**Packet**發送時的資料。



Point to Point Tunneling Protocol (PPTP) 原理

- PPTP是一個常用在VPN中的一個協定，藉由GRE header，將資料從IP packet換成PPP packet
- 加入連線認證機制，採用client-server模式，稱爲Enhance GRE



Point to Point Tunneling Protocol (PPTP)原理

- PPTP連線實例
- PPTP連線：
  1. 當PPTP Client A欲和PPTP Server B建立連線。
  2. PPTP Client A和PPTP Server B使用MS-CHAP來做連線認證。
  3. 當認證通過後，及建立一個PPTP Tunnel。
- PPTP傳送：
  1. 當Host A 要傳送Packet給在Network B的Host B。
  2. Host A將Packet送至PPTP Client A。
  3. PPTP Client A 將Packet包裝成PPP再加上GRE Header，經由Internet傳送至PPTP Server B。
  4. PPTP Server B將資料解封裝，經由Network B送給Host B。
  5. Host B接收到Packet並做出適當的回應。

Note: 身份驗證方法

- **CHAP**
  - CHAP 通過使用 MD5 來協商的一種加密身份驗證之安全形式
- **MS-CHAP (Microsoft Challenge Handshake 驗證通訊協定)**
  - 由微軟開發，爲了對遠端 Windows 工作站進行身份驗證
- **MS-CHAP v2**
  - 第二版的質詢握手身份驗證協議，它提供了相互身份驗證和更強大的初始資料密鑰，而且發送和接收分別使用不同的密鑰

Enhanced Generic Routing Encapsulation Header

- **PPTP Packet**
- **PPTP所使用的GRE Header**
  - **Key Payload Length :** 紀錄**GRE**封裝的**PPP Packet**的大小，但不包含**GRE Header**的長度。
  - **Key Call ID :** 包含這個連線的**Call ID**，用來分辨連線。
  - **Acknowledgment Number :**記錄著所接收的**Packet**中，最大的**Sequence Number**。

PPTP packet

Note:

- **IPSec（IP Security Protocol）**網際網路層安全協定

IPSec(1)

- **IPSec:**
  屬於IP Protocol的延伸，它提供了一個使用密碼將欲傳送的Packet加密的一種服務，使任何的IP protocol能夠使用一個”加密”的Tunnel。
- **IPSec**在傳送的方法
  - **Host-to-Host**
  - **Host-to-Network**
  - **Network-to-Network**
- **IPSec**的「安全」
  - 資訊的機密性（**Confidentiality**）：避免被竊聽
  - 資料的一致性（**Integrity**）：保證內容不被篡改
  - 資料來源的驗證（**Authentication**）：確保資料並非由網路上的第三者所假造

IPSec(2)

- Authentication Header (AH):
  記錄著Data加密的雜湊(hash)資訊，以及識別資訊，用來確保IP Packet在傳送的時候不被修改。
- Encapsulation Security Payload (ESP)：
  對Datagram做加密用的，保護IP Packet，當Packet被竊聽，解開Packet以後，ESP能夠確保內容不被解讀出來。

IPSec(2)

- IPSec連線模式:
  - **Transport Mode** :有關Security的Header紀錄在Transport Layer Header，在IP Header加入Packet之前就被加入。IPSec會利用AH或ESP對Packet做加密的的動作。
  - **Tunnel Mode** :使用AH和ESP將整個欲傳送的IP Packet加密，並且再加上一個新的IP Header，才將Packet傳送到接收端。

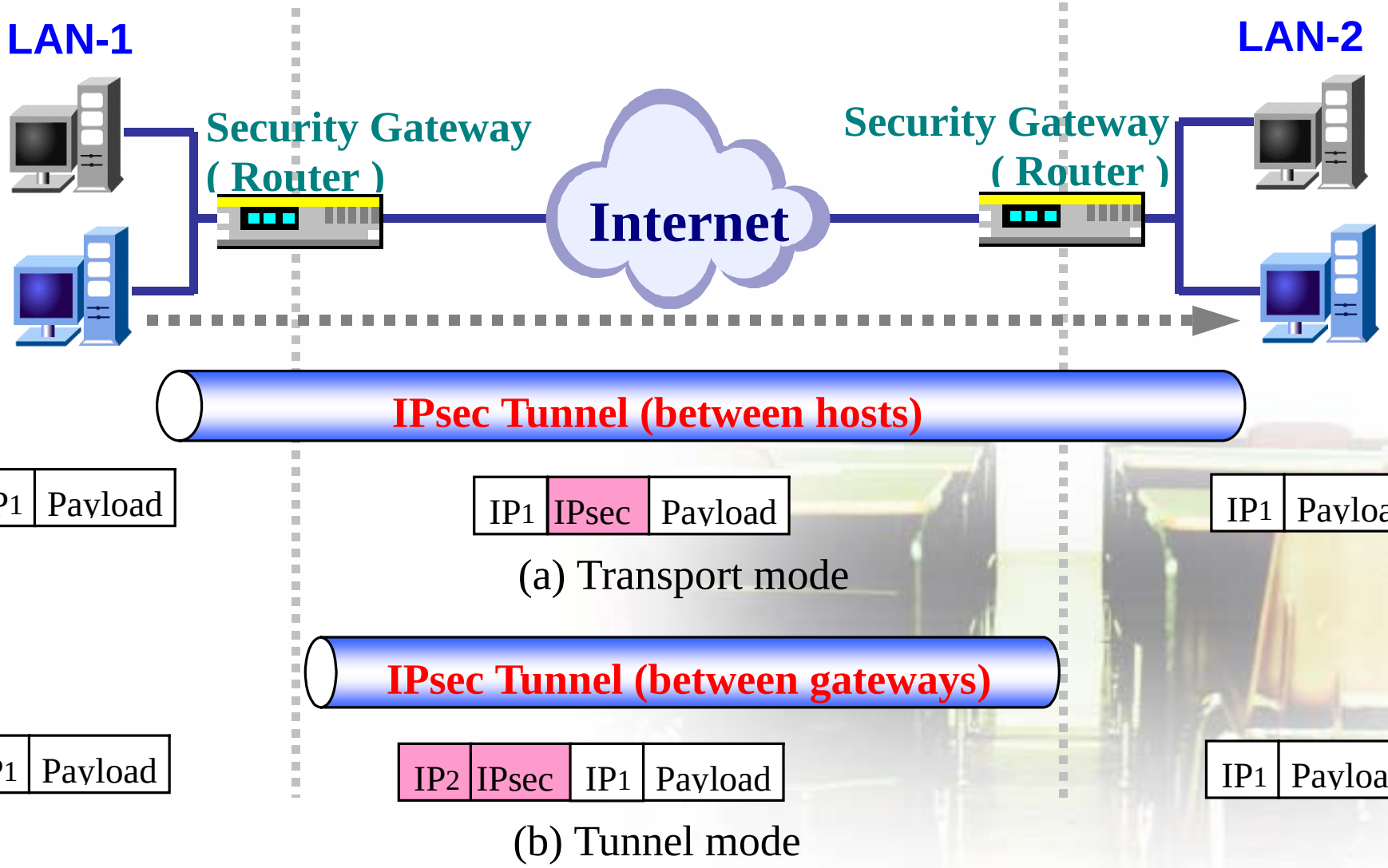
IPSec(3)

- **Transport Mode上的Packet格式：**

IP Header
AH
ESP
TCP Header
Data

- **Tunnel Mode的Packet格式:**

IP Header 2
AH
ESP
IP Header 1
TCP Header
Data


LAN-1
LAN-2
Security Gateway
(Router)
Internet
Security Gateway
(Router)
IPsec Tunnel (between hosts)
IP1 Payload
IP1 IPsec Payload
IP1 Payload
(a) Transport mode
IPsec Tunnel (between gateways)
IP1 Payload
IP2 IPsec IP1 Payload
IP1 Payload
(b) Tunnel mode

- **Transport Mode的封包轉換過程**
  IP封包經過IPsec的處理後、僅在原有的IP Header之後插入適當的IPsec Header，此法對原封包的資料量擴充較少，而且封包一出主機即保證安全，缺點是每台主機都需要裝設IPsec。
- **Tunnel Mode封包的轉換**
  因Security Gateway必須在原IP封包之外再包一個IP Header（來源端位址是Gateway自己、目的位址則是遠端的Gateway），所以封包的擴充量較大，而且在區域網路內，真正的通訊主機和Gateway之間完全無安全保護。但Tunnel Mode的好處是在原本區域網路內部所有主機、應用軟體皆不須更動的狀況下，每個區域網路僅需在對外的Router上裝設IPsec，使LAN到LAN之間跨越Internet的部份用IPsec保護連線，即可建置出安全的的VPN Tunnel。

IPSec的協定

- 若從功能面來看，**IPSec**包含了三種協定，分別提供不同的功能
  - 金鑰交換協定：負責建立安全聯結與交換金鑰。
  - 認證表頭 (Authentication Header，AH)：主要提供認證的功能。
  - 資料封裝加密 (Encapsulating Security Payload，ESP)：主要提供加密的功能，也可選擇性地再加上認證的功能。

- 金鑰交換協定主要負責這兩項工作：
  - 建立安全聯結。
  - 建立共同的秘鑰。
- **IPSec目前預設的金鑰交換協定為ISAKMP (Internet Security Association and Key Management Protocol)與Oakley。Oakley僅規定金鑰交換的方法，至於各種訊息詳細的格式則是由ISAKMP所定義。ISAKMP同時也規定了安全聯結的建立步驟。ISAKMP/Oakley協定相當複雜，因此僅大略介紹其原理與功能。其他部分請自行參考RFC文件。**

❖安全聯結具有單向的特質

- 即當A傳送資料給B時需定義一項安全聯結，而B傳送資料給A時需要另一組安全聯結

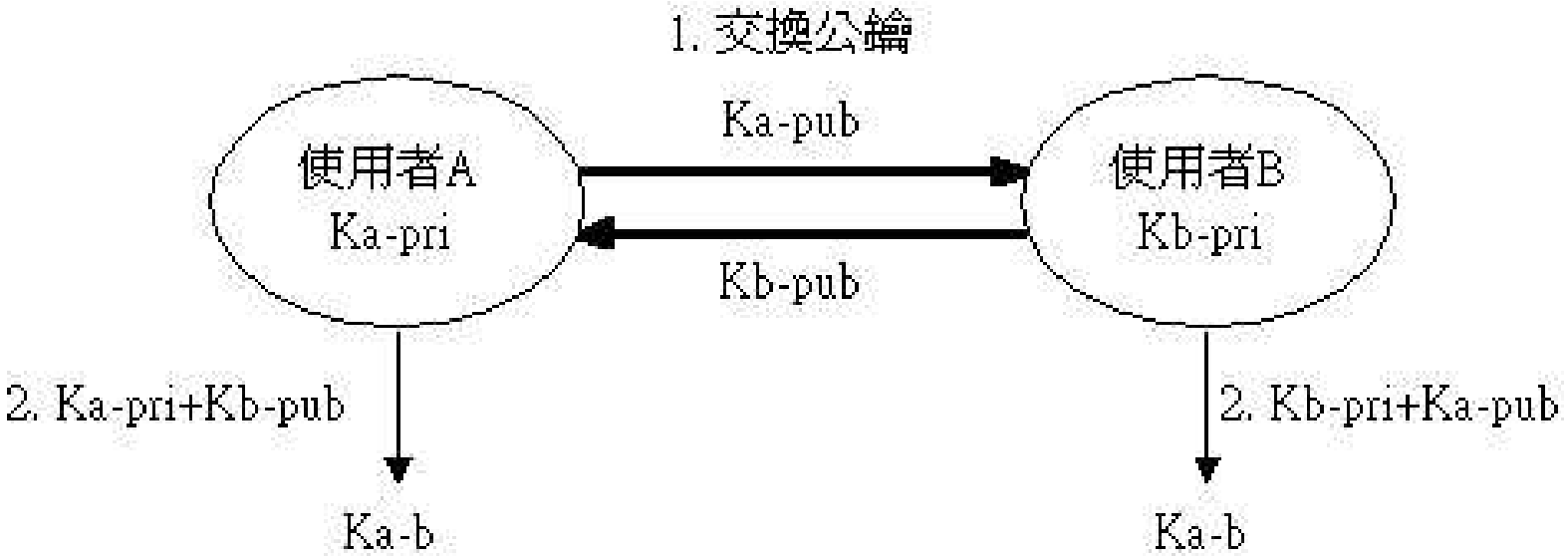
❖安全聯結中有三個最重要的參數：

- Security Parameters Index (SPI，安全係數索引)：SPI是由IPSec接收端在自行定義的數值，長度爲32位元，會記載於每個IPSec封包中。例如，A、B、C同時要以IPSec傳送資料給X，則X會定義三個SPI值，之後便可利用IPSec封包中的SPI欄位，辨識該封包隸屬哪個安全聯結。
- Security Protocol ID(安全協定ID)：指定要使用AH或是ESP表頭。每項安全聯結僅能在AH或ESP中擇其一。因此，若要同時使用AH與ESP來傳輸資料時，則必須用到兩項安全聯結；若要同時使用AH與ESP建立雙向傳輸關係，則需要四項安全聯結。
- IP destination address (IP目的位址)：安全聯結的單方關係是以接收端的IP位址來定義

金鑰交換的原理

❖ IPSec所使用的Diffie-Hellman金鑰交換法

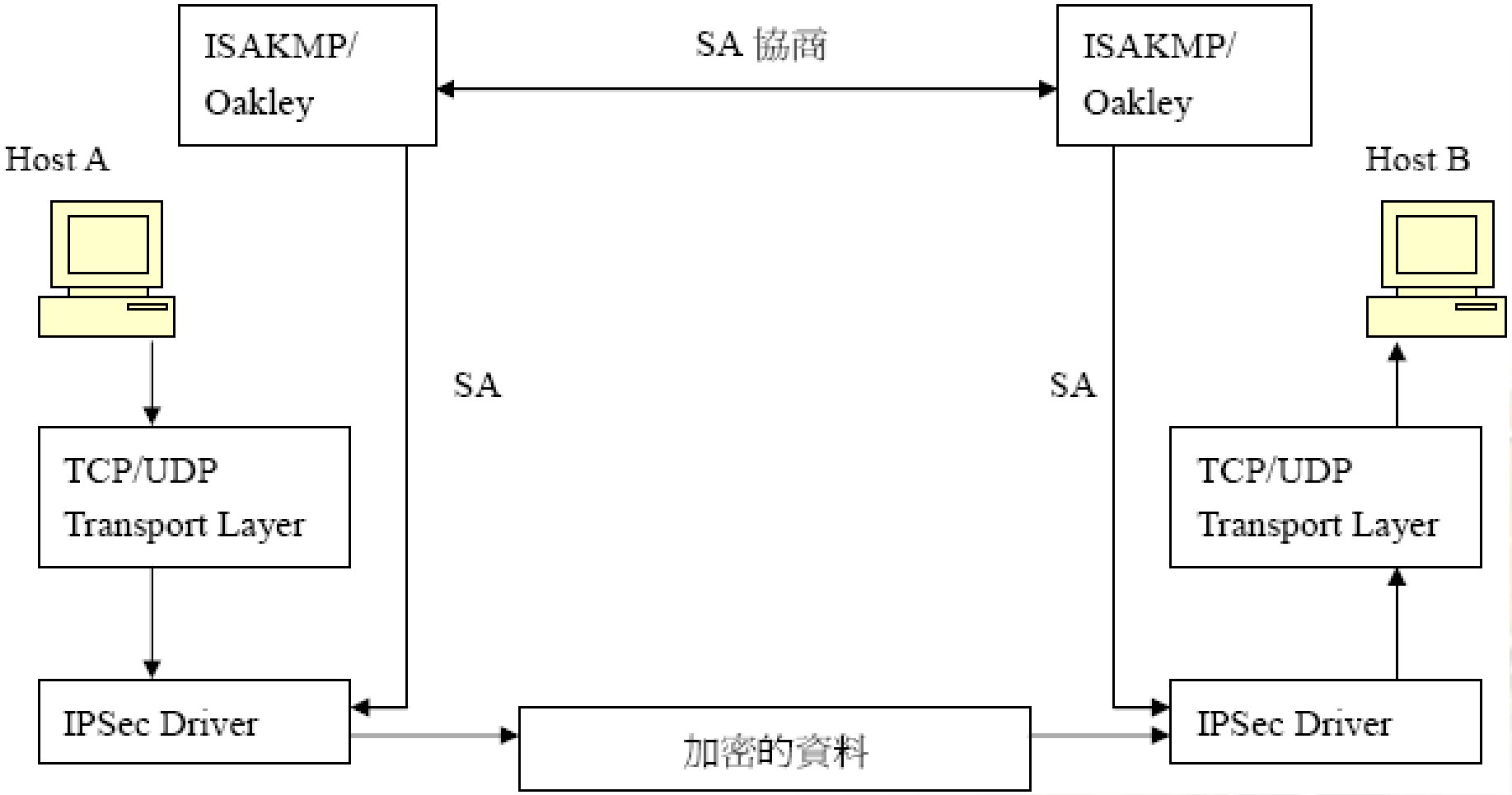
- 雙方先以非對稱式加密法來交換彼此的公鑰(Ka-pub與Kb-pub)。
- 再以對方的公鑰與自己的私鑰，運算求得一把共同的秘鑰(Ka-b)。
- 利用秘鑰以對稱式加密法，來進行加密或認證的動作。



- 在後續的加密過程中，若反覆使用同一把秘鑰，比較容易被人破解。爲了提高加密安全性，秘鑰每隔一段時間便會重新建立，這種秘鑰就稱爲階段金鑰或工作金鑰**(Session Key)**。這也是爲什麼安全聯結必須定期重新協調的主要原因。

IPSec(4)

❖ IPSec實做流程圖



IPSec(5)

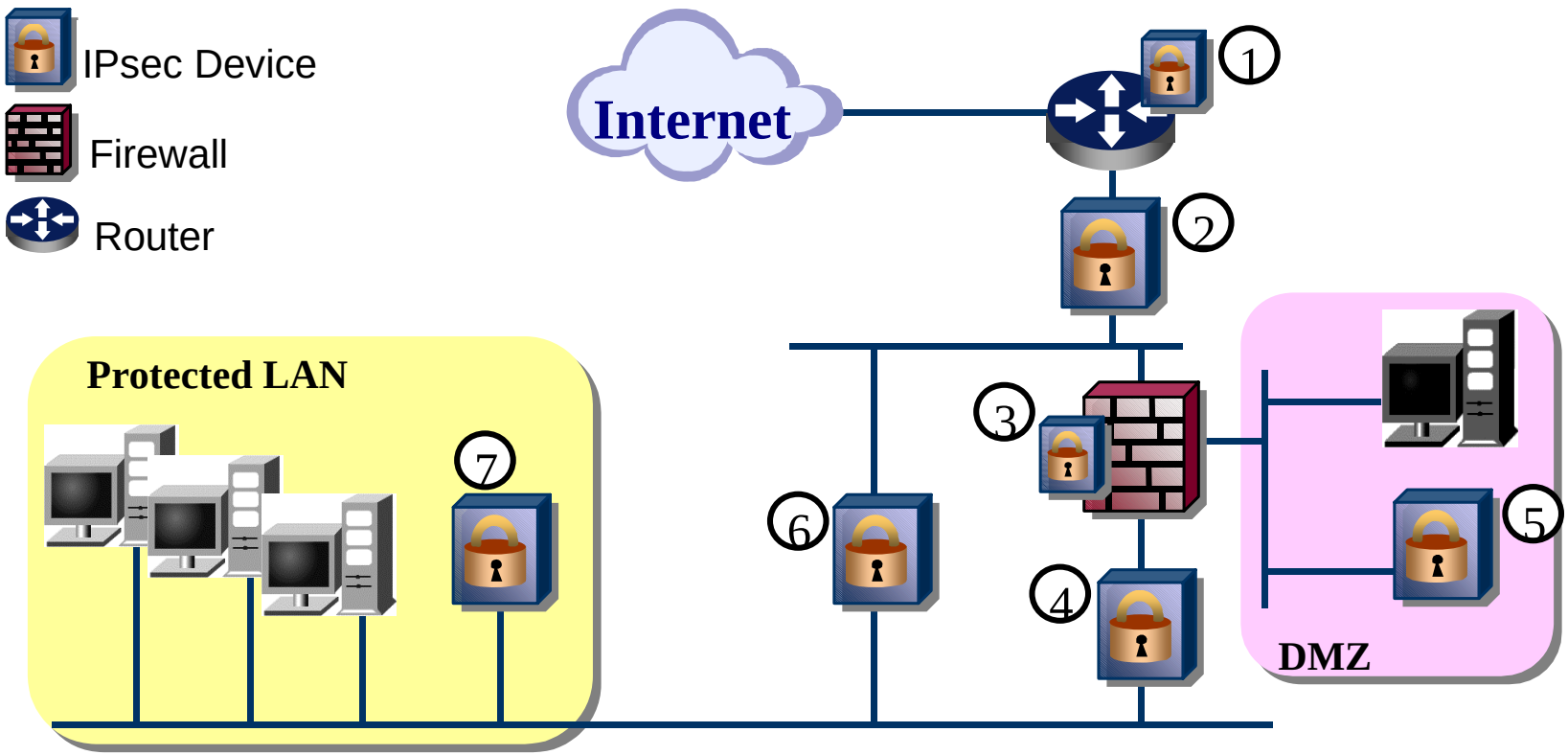
- IPSec實做過程:
- IPSec連線建立:
  1. SA協商。
  2. 兩者協商Key的交換以及管理方式。
  3. 協商成功後，IPSec連線建立。
- IPSec資料傳送:
  1. Host A欲傳送Packet給Host B
  2. Host A將Packet產生，並由IPSecDriver將Packet加密。加上AH和ESP Header。
  3. 將IP Header加上並將這個加密過的Packet經由網路送至Host B
  4. Host B使用共同協商過的Key將Packet解密。
  5. Host B收到原始的Packet並產生應有的回應。

IPsec與Firewall

- 防火牆（**Firewall**）的主要工作是在控管、阻絕內部網路以及外部網路間的資料交換，以防止未經授權（允許）的網路連線。依照**Firewall**的運作原理，至少可區分爲**Packet-based Firewall**、**Application Layer Firewall**、及**Stateful Inspection Firewall**。這些**Firewall**在實作難度與成本、執行效能、管理難易、以及防護能力上皆各有所長，須視用戶的需求而選擇適當的**Firewall**。而**Firewall**在網路上的裝設位置，依其運作原理及所要保護的網路範圍而有不同，也因此有所謂的**Dual-homed Host Firewall**、**Screened Host Firewall**、**Screened Subnet Firewall**等等不同形式。

- 不管是哪種類型的**Firewall**，現今所有的區域網路都至少會擇一裝設，達成最基本的安全保護。
- **Question:**
  在已有**Firewall**的狀況下，**IPsec VPN**設備應該設置於何處，才能提供安全可靠的**VPN**服務，同時又不損害**Firewall**原有的保護機制？

- 這個問題並沒有唯一的答案。在一個由**LAN**、**Firewall**、**Server**、**Router**所組成的標準企業網路中，**IPsec Device**至少可以有**7**種安置模式，而這些模式皆有其優缺點，須視企業用戶的需要而定。


IPsec Device
Firewall
Router
Internet
Protected LAN
DMZ
1
2
3
4
5
6
7

- 模式一：Router提供IPsec服務
  現今已有許多大、小型Router直接將IPsec加入，他的好處是不須另外購置IPsec Device，而且因爲在Firewall的保護之外，因此很容易透過Internet直接由遠端做控制，且對用戶而言，內部原有網路幾乎完全不須更動。其缺點是Router的執行效率會大受影響，而且IPsec本身的設計即易受DoS（Deny-of-Service）的攻擊，此種架構將使Router易因IPsec受攻擊而停擺，使得企業網路聯外的可使用性大打折扣。

- 模式二：IPsec Device建置於Firewall之外
  這種模式的好處是Router與Firewall都可沿用舊有的設備、減輕Router的負擔。但是未受保護的IPsec Device一樣易受DoS攻擊；而且，如果進入的封包必須做IPsec保護但未做，因爲Firewall收到的都是已解除IPsec的原始封包，因此無從辨識起，除非IPsec Device自身具備Packet Filter的功能而能拒絕該封包進入；另一個問題是IPsec Device是純IP的機制，如果內部網路也接受non-IP的封包進入，則必須設法繞過IPsec Device。

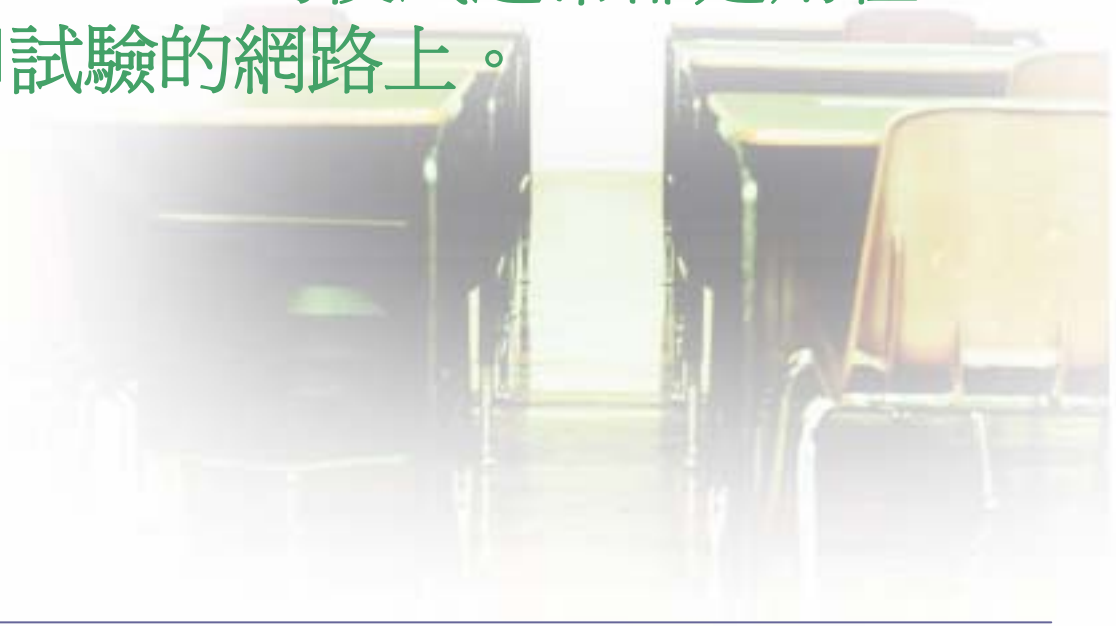
- 模式三：Firewall提供IPsec服務
  此模式恰能解決模式二IPsec Device需要Packet Filter的問題，且安全控管的工作集中在同一平台下也易於管理，目前已有許多Firewall產品宣稱提供額外的VPN服務，即是此種模式。然而，過去Firewall爲了強化其本身的安全性，因此多要求Firewall設備必須「簡單」、盡量減少不必要的服務，複雜的IPsec加入Firewall後恰好與此原則相衝突，因此也有網路安全專家建議應該將IPsec Device與Firewall分開設置。

- 模式四：IPsec Device建置於Firewall之後透過Firewall的保護，可以減少IPsec Device遭受DoS攻擊，同時可減輕Firewall的負擔。但是，因爲Firewall收到的外來封包都是未經解密的IPsec封包(如Tunnel Mode)，Firewall無從知道內部封包的真正來源與目的地，所以無法達成有效的封包管控的目的，因此，該封包通過IPsec Device解密後，必須再透過Packet Filter的機制、再做一次封包管控的工作。此模式的另一個缺點是現今許多Firewall都同時提供NAT的功能，這種先做IPsec再做NAT的方式將難以實作。

- 模式五：IPsec Device建置於DMZ(De-Militarized Zone，隔離區)內
  就如同一般企業網路會將某些伺服器設置在Firewall的DMZ之中一樣，此時IPsec封包會先經由Firewall的過濾再送往IPsec Device解密、再經過Firewall做一次原始封包的過濾，最後才傳送給LAN。因此IPsec Device本身及加解密前後的封包皆受到Firewall的嚴密管控，但是相對的缺點即是Firewall的負擔極爲沈重，且Firewall必須識得IPsec格式的封包，才能正確處理，因此舊有的Firewall將可能無法繼續使用。

- 模式六：IPsec Device與Firewall平行建置
- 當封包經由Router進來時，Router必須先分辨封包格式，IPsec封包則丟往IPsec Device，non-IPsec或non-IP封包則丟往Firewall處理。此法的好處是原有舊的Firewall可繼續使用、內部網路可同時支援IP/non-IP封包格式。但是，Router必須懂得分辨IPsec封包，而IPsec Device不僅未受Firewall保護，本身還須具備Packet Filter功能（如模式四）；一個問題則是，原本需要做IPsec保護才可送出的封包，可能直接經由Firewall、未加密保護即送出去，造成安全漏洞。

- 模式七：**VPN-on-a-stick**
  此種模式只是在**LAN**增設一台**IPsec Server**，因此正確的封包**Routing**很是重要，否則封包可能未經保護即丟往**Internet**。而且因爲同一個封包會在**LAN**上出現兩次，會造成網路的負擔。所以，**VPN-on-a-stick**的模式通常都是用在小型、或是做**VPN**試驗的網路上。

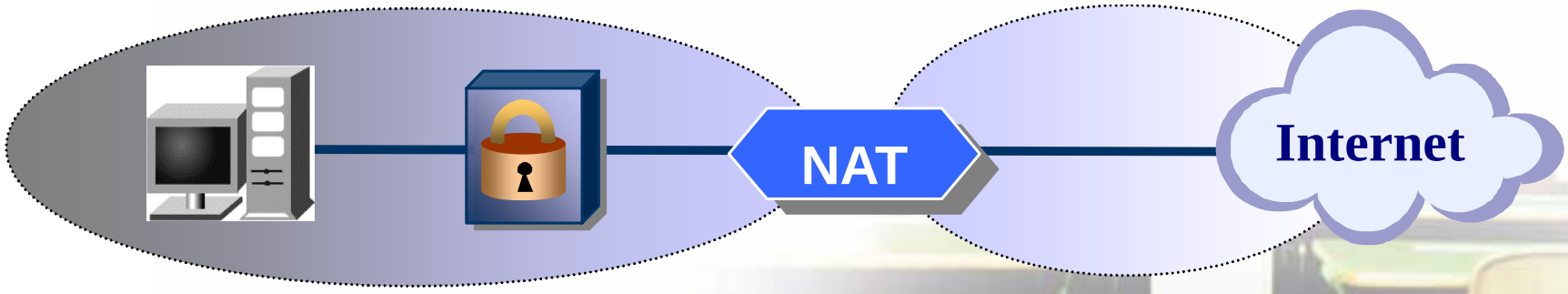


IPsec與NAT

- 由於近來公用IP Addresses已經不敷使用，一般企業網路多是利用NAT（Network Address Translation）的技術來使多個私有IP Addresses共享少數（或單一）的公用IP。其實NAT是一對一的靜態對映的NAT與多對一的動態對映的PAT的統稱，大致的做法是：當一個封包由內部網路往外傳送時（此時IP Header的Source IP是原有的私有IP address），NAT Device會選取一個可用的公用IP（及Port Number）取代封包中的Source IP（與Port），同時修正TCP/UDP Header中的Checksum內容（因爲此值與IP Header內容有關），再把封包往Internet送。

IPsec與NAT

- 當一個系統必須同時採用IPsec與NAT時，通常只有兩種結合模式：先做IPsec再做NAT，或是做NAT再做IPsec。



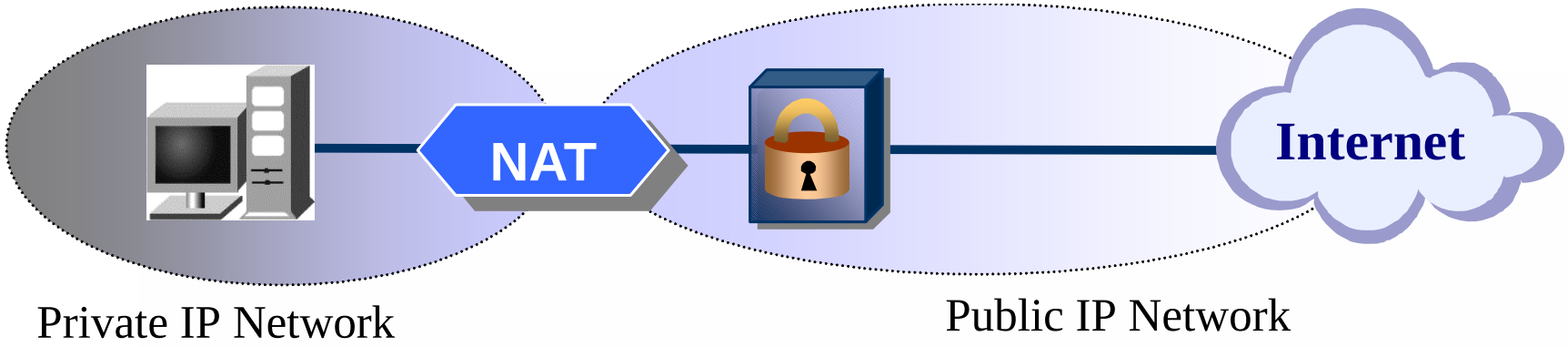
圖四、先 IPsec 後 NAT 的結合模式

模式一：先IPsec再NAT

- 封包傳送前，先做**IPsec**的加密等封裝工作，再進行**NAT**的**Source IP/Port**的轉換。此時依**IPsec**所執行的協定不同會造成不同的結果：
  - [IPsec-AH + NAT]：由於IPsec的AH Tunnel/Transport Mode會針對整個封包(包括IP Header及Data Payload)做資料完整性的檢查，因此，當作完IPsec-AH、又再執行NAT的Source IP/Port轉換後，此封包在抵達遠端的IPsec Device時，AH的檢驗必定失敗，因此IPsec-AH + NAT的結合方式將無法運作。
  - [IPsec-ESP-Transport + NAT]：IPsec的ESP一樣支援資料完整性的檢查，但只針對Data Payload，因此封包經過NAT轉換IP/Port後，在遠端的IPsec Device做資料完整性檢查時並不會有影響。但ESP還會針對Data Payload做加密保護，因此，NAT無法在做完IP/Port的轉換後同步修改TCP/UDP Header內的Checksum值，使得遠端的Checksum檢驗仍舊會失敗。因此IPsec-ESP-Transport + NAT的結合方式將無法運作(除非遠端事先取消TCP/UDP Checksum的功能)
  - [IPsec-ESP-Tunnel + NAT]：類同於ESP-Transport Mode，在遠端的IPsec檢查亦會成功，而且之後的Checksum檢查也會通過。這是因爲IPsec Tunnel Mode是在原封包之外再新加一個IP Header，因此NAT只改到IP2，原IP Header(IP1)並未更動，所以最後的TCP/UDP Checksum檢查不受影響。
    雖然本模式容許IPsec與NAT並存，但仍有些問題：例如，因爲IP1是私有IP Address，因此遠端勢必須先了解我端的私有網路的建置，這種狀況在某些應用是不被允許的（如遠端是另一家公司的網路）。

模式二：先NAT再IPsec

- 封包要去前，先進行NAT的Source IP/Port的轉換，再做IPsec的加密等封裝工作。因NAT已經先完成所有封包轉換的工作，故IPsec任何加密或是資料完整性檢查皆不受影響。本模式的缺點是IPsec Device可能無法得知躲藏在NAT之後真正的封包來源，因Source IP都已被NAT轉換成公有IP Address(除非NAT已經事先做好一對一的靜態對映、並通知IPsec)。而且因爲IPsec Device身在Public IP Network，本身亦須要公用IP Address，所以，使用此模式的企業網路必須事先取得較多的公用IP。一種可行的解決方式是將NAT與IPsec建置在同一個設備中，透過統一的管理界面，IPsec可輕易取得NAT的IP對應方式，達到較具彈性的VPN服務。或是乾脆捨棄NAT，直接透過IP Tunnel Mode將私有IP的封包封裝成公用IP(但前提是遠端亦須知道我端的私有IP網路設定)



圖五、先 NAT 後 IPsec 的結合模式

- IPsec技術的提出雖然提供了網路通訊許多很好的安全保護，例如內容的保密、來源的驗證、避免篡改假造等，然而，其運用密碼學的特性也造成與現有其他安全機制相容的問題。在這篇文章中，我們先是討論了IPsec與Firewall合併使用的各種可能性。基本上，Firewall與IPsec並無相容性的問題，而只是在於企業網路基於設置成本、安全特性、管理難易等考量，需要何種整合的解決方案？
- 我們則討論了IPsec與NAT「不」相容的問題，目前各個網路設備大廠（如Cisco）也在IETF提出有關解決兩者合用的方法，但目前尚無一勞永逸的方案出現。因此我們的建議是，要不就不使用NAT，若需要NAT，建議採用先NAT再IPsec的方式（第四節、模式二），尤其若能採用合併成同一設備的方式，則可達成更好的管理彈性。