

**國家資通安全防護整合服務計畫
網路架構規劃參考指引
(V3.1)**

行政院資通安全會報技術服務中心
中華民國110年12月修訂

修訂歷史紀錄表

項次	版次	修訂日期	說明
1	V1.0		新編
2	V2.0	107/1/12	<ol style="list-style-type: none">1. 修正適用對象2. 將 2.2.1 TCP/IP 與 DoD 四層模型移至 2.1.2，並增列 DoD 四層模型之來源3. 增列 2.3.5 入侵偵測防禦系統之節次，並說明其與 Firewall 之關聯4. 於常見錯誤樣態之備註欄說明參閱之章節
3	V3.0	108/6/12	修正引用 ISO/IEC 7498-1:1994 標準 OSI 參考模型與參考文獻：
4	V3.1	110/12/31	修正引用資通安全事件通報及應變辦法

報告摘要

報告名稱	網路架構規劃參考指引
資訊等級	<input type="checkbox"/> 機密 <input type="checkbox"/> 密 <input type="checkbox"/> 內部使用 <input checked="" type="checkbox"/> 普通
相關撰稿人	江衍勳、林子群、王智民、陳相武、孫立勇、鍾榮翰
閱讀對象	<input checked="" type="checkbox"/> 一般主管 <input checked="" type="checkbox"/> 資安人員 <input checked="" type="checkbox"/> 資訊人員 <input type="checkbox"/> 一般使用者
<p>內容摘要：</p> <p>行政院歷年辦理資安稽核工作，過程中經常發現機關之網路架構圖，不符合其拓樸(Topology)架構、路由表設定錯誤、防火牆配置不當等設定錯誤情況，衍生安全疑慮，故編撰本指引提供機關參考，以協助機關於規劃建置網路架構時，全面性的檢視各種架構與資安上所需考量的重點，同時也提供常見之錯誤樣態，讓機關人員檢視現行架構中是否存在相同或類似的問題，並針對現行架構進行改善，進而提高網路服務的可靠度與安全性。</p> <p>本指引主要章節區分為前言、技術架構、管理程序、實務範例、參考文獻、網站資源表列及附件等 7 章，針對網路架構規劃提供具體建議，包含網路架構之技術簡介、運作原理及安全技術等，並針對建置過程之管理程序，包含「規劃」、「執行」、「檢查」、「行動」各階段之注意事項，提供具體建議。</p> <p>技術架構是針對本指引使用的相關技術進行說明，同時也針對運作原理進行整理彙整，提供機關人員參考，另外也針對相關原理的安全技術進行整理分析，並說明網路部署原則，同時亦針對資安健診服務常見之錯誤樣態加以彙整，提供機關執行資安稽核作業之參考，另提供實務案例說明，可參考其他機關之規劃情形，並提供實務之具體建議。</p>	
關鍵詞	網路架構、拓樸、DNS、DMZ

目 次

1. 前言	1
1.1 目的	1
1.2 適用對象	1
1.3 章節架構	4
1.4 使用建議	5
2. 技術架構	6
2.1 技術簡介	6
2.2 運作原理	24
2.3 安全技術	41
2.4 部署原則	57
3. 管理程序	75
3.1 「規劃」	75
3.2 「執行」	94
3.3 「檢查」	97
3.4 「行動」	97
4. 實務範例	98
4.1 實務範例(一)	98
4.2 實務範例(二)	98
5. 參考文獻	99
6. 網站資源表列	100
7. 附件	101
附件 1 「網路架構規劃」安全控制措施查檢表	附件 1-1
附件 2 機關導入完整報告(一)	附件 2-1
附件 3 機關導入完整報告(二)	附件 3-1
附件 4 專有名詞中英對照表	附件 4-1
附件 5 導引手冊 Quick Guide	附件 5-1

圖目次

圖 1	OSI 參考模型.....	6
圖 2	OSI 模型說明.....	7
圖 3	實體層資料傳輸.....	8
圖 4	資料連結層資料傳輸.....	10
圖 5	網路層資料傳輸.....	11
圖 6	傳輸層資料傳輸.....	13
圖 7	路由器間對應的層連線.....	15
圖 8	匯流排拓樸架構.....	18
圖 9	星狀網路架構圖.....	19
圖 10	樹狀網路架構圖.....	20
圖 11	網狀拓樸架構.....	21
圖 12	混合式拓樸架構.....	22
圖 13	SNMP Manager 與 Agent 的溝通指令.....	31
圖 14	管理資訊庫的樹狀結構圖.....	33
圖 15	機關網路防火牆樣態.....	42
圖 16	IEEE 802.11 安全防護技術架構.....	49
圖 17	IEEE 802.11 安全使用之加密演算法.....	49
圖 18	802.11 安全性機制發展歷程.....	50
圖 20	機關區域劃分圖.....	59
圖 21	機關區域存取控制圖.....	66
圖 22	機關邏輯網路架構圖(範例).....	68
圖 23	機關實體網路架構圖(範例).....	69
圖 24	DFD 背景圖範例.....	78
圖 25	第 0 階資料流程圖範例.....	79
圖 26	機關網路架構檢核導入流程圖.....	82
圖 27	機關核心系統 DFD 繪製圖.....	95
圖 28	機關核心系統存取控制檢核.....	96

表 目 次

表 1	網路架構規劃參考指引適用對象對照表	2
表 2	WPA 針對 WEP 安全弱點的因應方案	53
表 3	機關 VLAN 網段位置整理(範例)	61
表 4	A 機關負載平衡器	63
表 5	A 機關對 B、C、D 機關防火牆	63
表 6	A 機關核心交換器 VLAN 網段 IP 與路由	64
表 7	機關網路架構常見錯誤樣態	71
表 8	機關存取控制常見錯誤樣態	72
表 9	網路備援常見錯誤樣態	72
表 10	機關防火牆常見錯誤樣態	73
表 11	網路傳輸常見錯誤樣態	74
表 12	資料流程圖之符號說明	76

1. 前言

1.1 目的

資安會報自 102 年起推動政府機關資安健診服務，透過整合各項資訊安全項目的檢視服務作業，提供受檢機關資安改善建議，以落實技術面與管理面相關控制措施，提升網路與資訊系統安全防護能力。其中有關網路架構檢視，係針對網路架構圖進行安全性弱點檢視，檢視之項目包含設計邏輯是否合宜、主機網路位置是否適當及現有防護程度是否足夠等。

資安會報辦理資安稽核作業，由技服中心進行技術檢測，檢測過程中經常發現機關之網路架構規劃，不符合其拓樸(Topology)架構、路由表設定錯誤、防火牆配置不當、誤將提供內部使用之網域名稱伺服器(DNS)錯植於DMZ(網路非軍事區)等設定錯誤情況，衍生安全疑慮，故於 105 年編撰「路由表設定、DNS 設定、防火牆設定及網路拓樸架構簡易說明手冊」。

復因為充實前述簡易手冊之內容，於 106 年編撰「網路架構規劃參考指引」，提供機關網路架構規劃之參考，協助機關於規劃建置網路架構時可參考本指引，進而更全面性的檢視各種架構與資安上所需考量的重點，同時亦提供常見之錯誤樣態，讓機關人員得以檢查現行架構中是否存在相同或類似的問題，能夠針對現行架構進行改善，進而提高網路服務的可靠度與安全性。

1.2 適用對象

本指引適用於政府機關運用資訊科技從事「業務維運」之相關人員，為便於閱讀與使用，特將適用對象區分為「一般主管」、「資訊人員」、「資安人員」及「一般使用者」，並針對不同對象建議閱讀之重點，適用對象對照表，詳見表 1 所示。

表1 網路架構規劃參考指引適用對象對照表

章	節	款	一般主管	資訊人員	資安人員	一般使用者
2. 技術 架構	2.1 技術簡介	2.1.1 網路 OSI 參考模型 2.1.2 TCP/IP 與 DoD 四層模型 2.1.3 網路拓模型態 2.1.4 軟體定義網路(SDN) 2.1.5 網路功能虛擬化(NFV)	△	○	○	
	2.2 運作原理	2.2.1 乙太網路 2.2.2 光纖網路(Fibre Channel) 2.2.3 路由協定 2.2.4 網路管理協定 2.2.5 防火牆運作原理 2.2.6 OpenFlow 傳輸協定 2.2.7 NFV 參考架構	△	○	○	
	2.3 安全技術	2.3.1 SNMP 安全性 2.3.2 Firewall 安全技術 2.3.3 DNS 安全性設定 2.3.4 DDoS 防禦技術 2.3.5 入侵偵測防禦系統 2.3.6 無線網路安全機制	△	○	○	
	2.4 部署原則	2.4.1 網路設備之組成 2.4.2 網路區域劃分 2.4.3 機關 IP、VLAN 及路由的劃分 2.4.4 核心系統資料流程圖繪製 2.4.5 機關區域間存取控制設定	△	○	○	

章	節	款	一般主管	資訊人員	資安人員	一般使用者
		2.4.6 繪製機關網路架構圖 2.4.7 網路架構探查的呈現與監控 2.4.8 比對檢核表，稽核檢測狀況 2.4.9 常見錯誤樣態與架構歸納				
3. 管理程序	3.1 規劃	3.1.1 導入前置需求 3.1.2 IP 設定與區域劃分 3.1.3 VLAN 與路由規劃 3.1.4 機關資料流程圖繪製 3.1.5 網路區域間存取控制 3.1.6 檢測流程規劃 3.1.7 檢測項目細項說明	△	○	○	
	3.2 執行	3.2.1 執行導入前置需求 3.2.2 確認 IP 設定與區域劃分 3.2.3 確認 VLAN 與路由 3.2.4 確認機關資料流程圖繪製 3.2.5 確認區域間存取控制 3.2.6 執行查檢表比對機關資料	△	○	○	
	3.3 檢查	3.3.1 檢查機關網路架構 3.3.2 檢查區域分隔與存取控制 3.3.3 檢查結果整理彙整	△	○	○	
	3.4 行動	3.4.1 矯正措施 3.4.2 預防措施	△	○	○	
	4.實務範例		△	○	○	
附	各項符號代表意義說明如后：					

章	節	款	一般主管	資訊人員	資安人員	一般使用者
記	○：詳閱；△：參考					

資料來源：本計畫整理

1.3 章節架構

本指引主要章節區分為前言、技術架構、管理程序、實務範例、參考文獻、網站資源表列及附件等 7 章，內容摘述如後：

第 1 章前言主要說明本指引編撰目的與適用對象，同時敘明本指引的章節架構，提供使用建議，讓政府機關運用資訊科技從事「業務維運」之相關人員，對管理目的及本指引架構能有全盤性的認知。

第 2 章技術架構是針對本指引使用的相關技術進行說明，同時亦針對運作原理進行彙整提供機關人員導讀，另外亦針對相關原理的安全技術進行整理分析，並於說明部署原則，讓機關人員能夠了解在規劃、建置網路時，所需的相關運作原理與安全技術，同時也知道部署時的原則及步驟。

第 3 章管理程序主要針對規劃、執行、檢查、行動等不同階段進行說明，提供機關人員實務上依循步驟，逐一確認注意事項，並透過本指引的建議，協助管理者達成規劃、執行、檢查、行動等不同階段的工作。

第 4 章實務範例，主要列舉導入機關的需要、過程、檢核的結果及專家顧問的建議，本章列舉 2 個導入機關實際導入案例，同時分析導入的過程與檢核結果，並提供實務建議。

第 5 章參考文獻主要說明本指引所參考的文獻資料。

第 6 章網站資源列表則列舉與本指引相關網站資料，提供機關人員參考運用。

第 7 章附件詳列本指引所納編之附件內容。

1.4 使用建議

本指引主要針對網路架構規劃提供具體建議，包含網路架構之技術簡介、運作原理及安全技術等，並針對建置過程之管理程序，包含「規劃」、「執行」、「檢查」、「行動」各階段之注意事項，提供具體建議。

同時針對資安健診服務常見之錯誤樣態加以彙整，提供機關執行資安稽核作業之參考。

另提供實務案例說明，可參考其他機關之規劃情形，並提供實務之具體建議。

機關可先參考附件 1，針對機關現行狀況進行檢核後，對於不符合項目，參考本指引相關說明執行安全控制措施，以強化機關資安防護。

2. 技術架構

2.1 技術簡介

2.1.1 網路 OSI 參考模型

ISO 於 1994 年發布 ISO/IEC 7498-1 標準，定義網路互聯的 7 層架構，也就是開放式系統互聯參考模型（Open System Interconnection Reference Model, OSI 參考模型），是一個認識網路架構非常好的模型，它定義了開放系統的階層、層次之間的相互關係及各層所包含的可能任務，作為一個架構來協調和組織各層所提供的服務，詳見圖 1 所示。摘述如後：



資料來源：本計畫整理

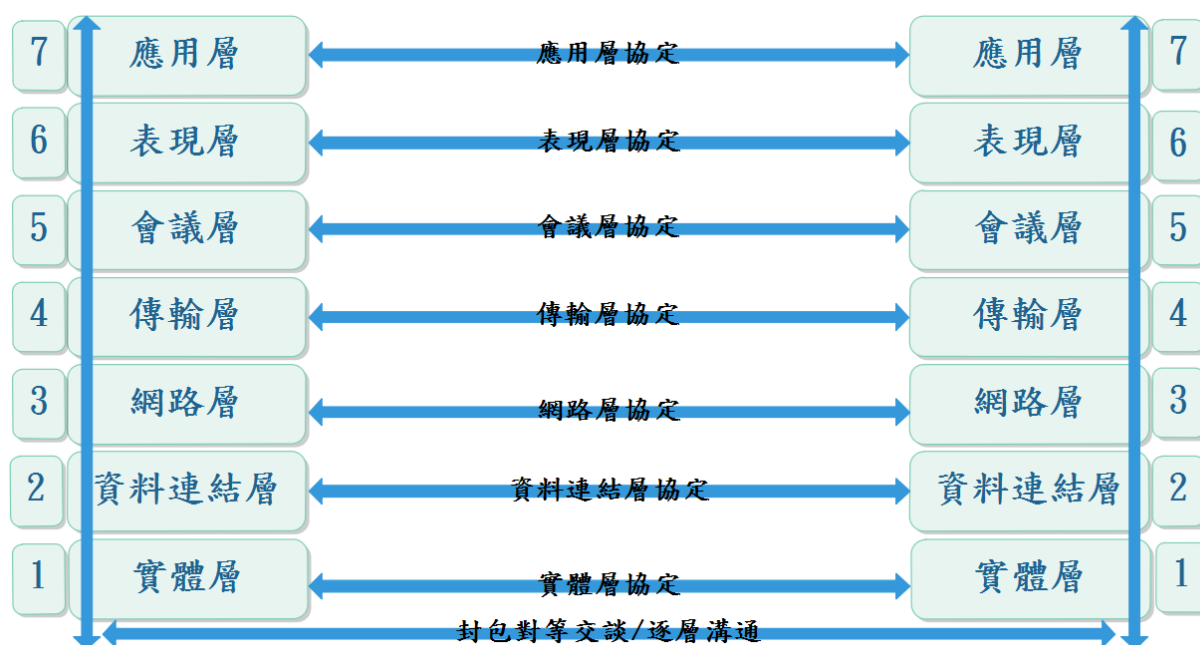
圖1 OSI 參考模型

在 OSI 7 層中，應用層是最接近使用者的層級，屬於此層的都是使用者較熟悉、可直接操作的軟體。而愈往下層則距離使用者的操作愈遠，反而與硬

體的關聯愈大。例如：資料連結層所負責的工作，幾乎都是由網路卡控制晶片和驅動程式來做；至於實體層的工作，那更是由硬體設備一手掌控，使用者完全無法干涉。

資料由傳送端的最上層(通常是指應用程式)產生，由上層往下層傳送。每經過一層，都會在前端增加一些該層專用的資訊，這些資訊稱為表頭(Header)，然後才傳給下一層，不妨將加上表頭想像為套上一層信封。

因此到了最底層時，原本的資料已經套上了 7 層信封。而後透過網路線、電話線、光纖等媒介，傳送到接收端，詳見圖 2 所示。



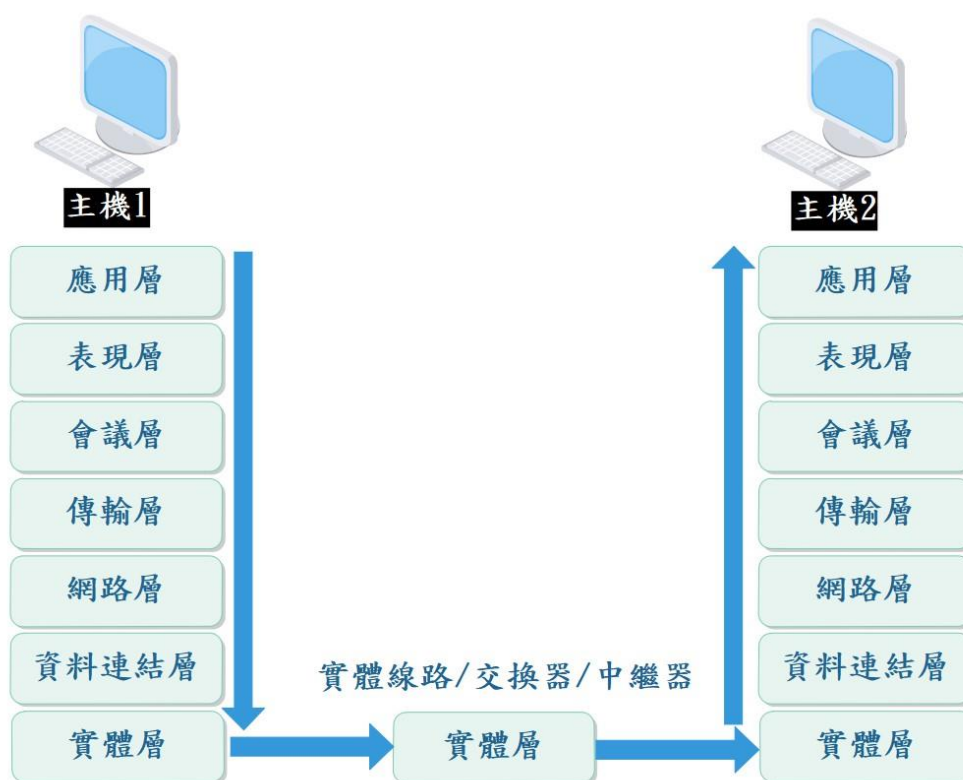
資料來源：本計畫整理

圖2 OSI 模型說明

2.1.1.1 實體層

實體層(Physical Layer)主要負責實體傳輸媒介規格訂定，無論何種通訊，最終得透過實體的傳輸介質來連接。所以數位資料在傳送之前，可能會經過轉

換，轉變為光脈衝或電脈衝以利傳輸，這些轉換及傳輸工作便是由實體層負責。此外，決定傳輸頻寬、工作時脈、電壓高低、相位等細節，也都是在此層規定，詳見圖 3 所示。



資料來源：本計畫整理

圖3 實體層資料傳輸

- 實體層包含：

例如纜線(Cable)、光纖(Fibre)、雙絞線(Twisted Pair)及連接端的規格，其中亦包含傳輸的訊號種類及轉換等。

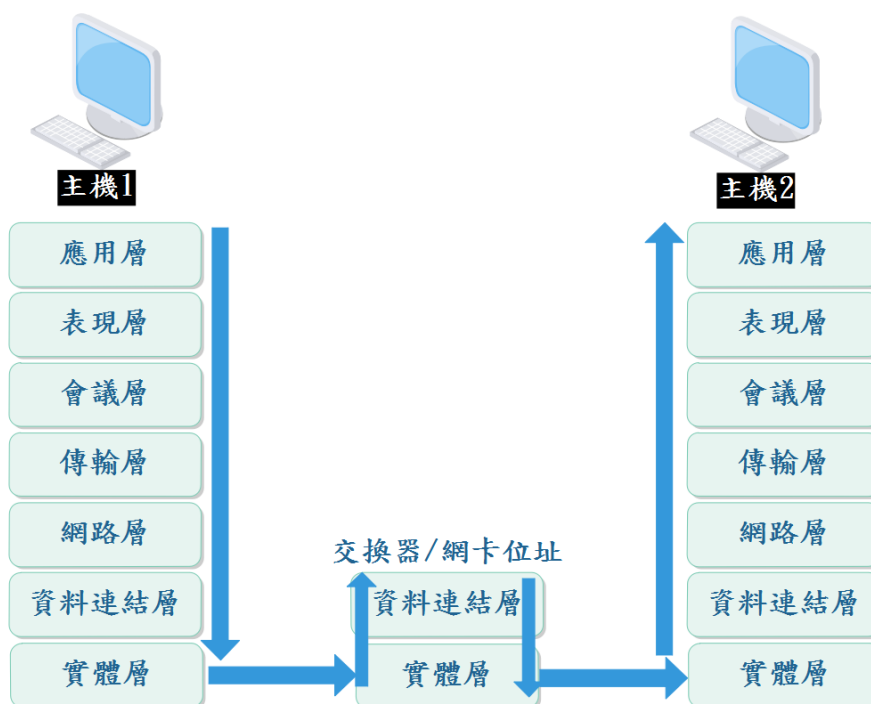
2.1.1.2 資料連結層

資料連結層(Data Link Layer)亦稱為資料鏈結層或鏈結層，是 OSI 參考模型第二層，位於實體層與網路層之間。在兩個網路實體之間提供資料連線的建

立、實際運作、結束的管理工作，也處理同步、偵錯、制定媒體存取控制的方法。

另外資料連結層亦定義構成資料傳輸資料單位(frame)並進行控制，作為傳輸過程中網路流量控制、錯誤檢測和錯誤控制等，控制傳輸流程的一端到另一端的資料傳輸。

資料連結層會在 frame 尾端放置檢查碼以檢查實質內容，檢查碼包含檢查位元(parity bit / check bit)、總和檢查(checksum / sum)及循環冗餘檢查碼 (Cyclic Redundancy Check Code, CRC)，將實體層提供的可能出錯的實體連線改造成邏輯上無差錯的資料封包，針對實體層的原始資料進行資料封裝。封裝資料資訊中，包含位址和資料等區段。位址段包含傳送點和接收節點的實體位址(如媒介存取控制(Media Access Control , MAC))，控制段用來表示連線封包的類型，資料段包含實際要傳輸的資料，詳見圖 4 所示。



資料來源：本計畫整理

圖4 資料連結層資料傳輸

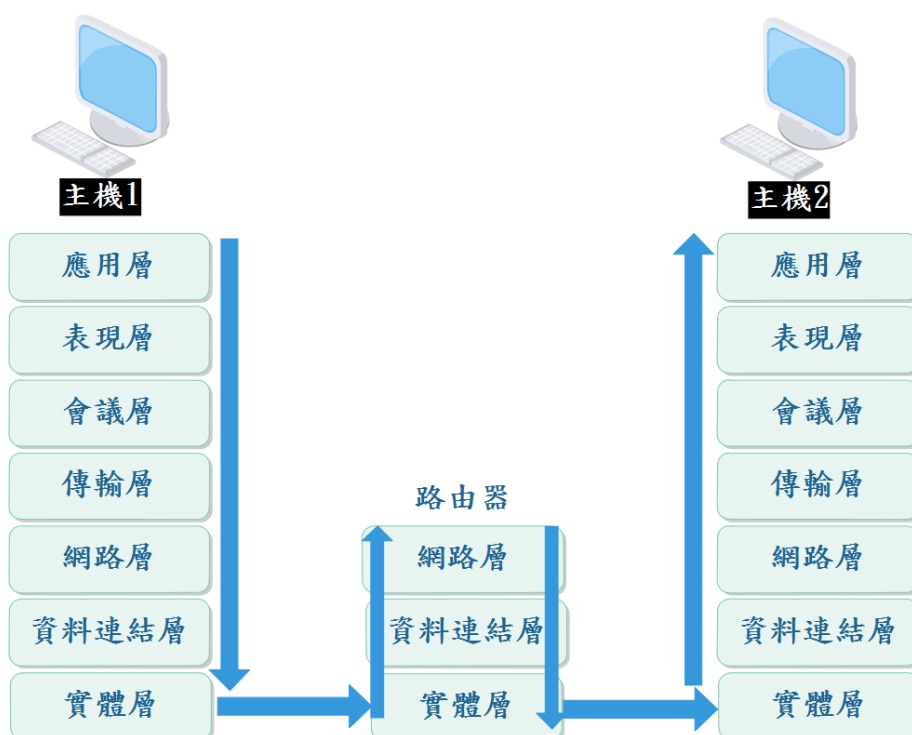
●資料連結層包含：

Wi-Fi(IEEE 802.11)、ARP(Address Resolution Protocol)、WiMAX(IEEE 802.16)、非同步傳輸模式(Asynchronous Transfer Mode, ATM)、數值地形模型(digital terrain model, DTM)、記號環網路(Token Ring)、乙太網路、光纖分散式數據介面(Fiber Distributed Data Interface, FDDI)、通用封包無線服務(General Packet Radio Service, GPRS)、EV-DO (Evolution-Data Optimized)、高速分組存取(high speed packet access, HSPA)、高級數據鏈路控制(high-level data link control, HDLC)、點對點協定(Point-to-Point Protocol, PPP)、PPPoE (Point-to-Point Protocol Over Ethernet)、L2TP(Layer 2 Tunneling Protocol)、整合服務數位網路(Integrated Services Digital Network, ISDN)、SPB(Shortest Path Bridging)、有遮蔽雙絞線(shield twisted-pair, STP)。

2.1.1.3 網路層

網路層(Network Layer)是 OSI 模型中的第三層(TCP/IP 模型中的網際網路層)。網路層主要提供路由和位址搜尋功能，使兩端點間能夠互相連線且尋找最佳路徑，同時具備針對擁塞和流量控制功能。由於 TCP/IP 協定中的網路層功能由網際網路協定(internet protocol, IP 協定)來實現，故又稱 IP 層。

在網路層中 IP 位址用來標識網際網路上的裝置，依靠 IP 位址進行相互通訊。在同一個區域網路中的內部通訊並不需要網路層裝置，依靠資料連結層就可以完成相互通訊，對於不同的區域網路之間相互通訊則必須藉助路由器等第三層裝置，詳見圖 5 所示。



資料來源：本計畫整理

圖5 網路層 資料傳輸

●網路層包括：

IP(v4·v6)、網際網路控制消息協定(Internet control message protocol, ICMP)、網際網路組管理協定(Internet group management protocol, IGMP)、IS-IS (Intermediate system to intermediate system)、網際網路安全協定(Internet Protocol Security, IPsec)、邊界閘道器協定(Border Gateway Protocol, BGP)、路由信息協議(routing information protocol, RIP)、開放最短路徑優先(open shortest path first, OSPF)、逆位址解析協定(Reverse Address Resolution Protocol, RARP)。

2.1.1.4 傳輸層

傳輸層(Transport Layer)主要針對連線的資料流支援、可靠性、流量控制等服務進行控制。在 OSI 模型中傳輸層常被稱作第 4 層或 L4，把傳輸表頭(TH)

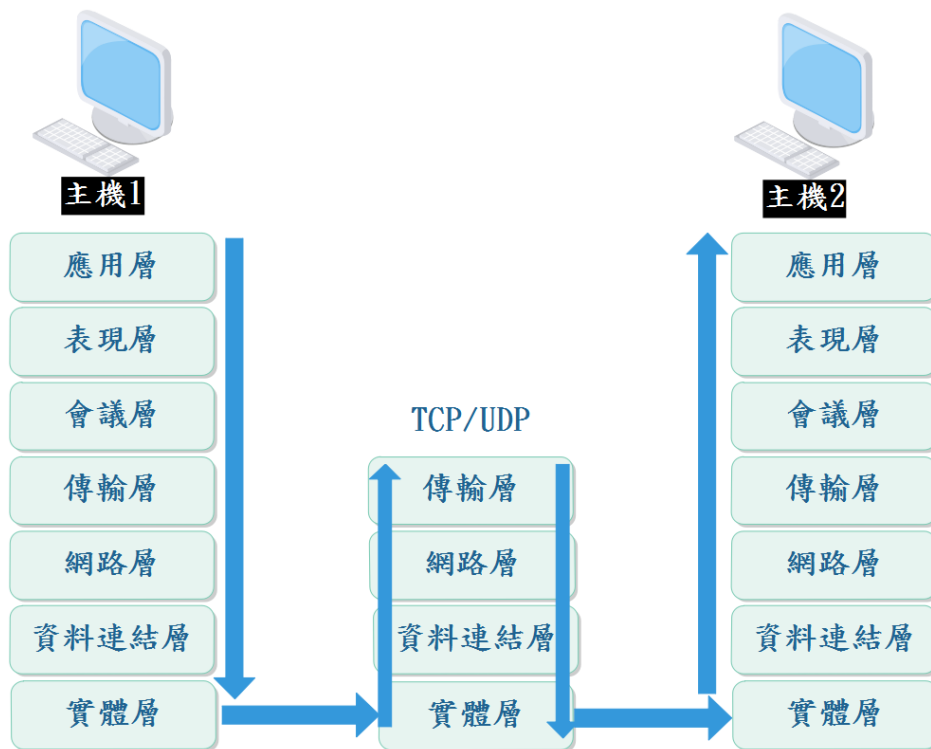
加至資料以形成資料封包。傳輸表頭包含所使用的協定等傳送資訊，例如：傳輸控制協定(transmission control protocol, TCP)等。

TCP 使用三向交握(Three-way Handshake)連線的傳輸，當用戶端試著與伺服器間建立 TCP 連線時，正常情況下用戶端與伺服器端交換一系列的資訊如後：

- 用戶端透過傳送 SYN 同步資訊到伺服器要求建立連線。
- 伺服器透過響應用戶端 SYN-ACK 以確認 (acknowledge) 請求。
- 用戶端答應 ACK，連線隨之建立。

這即是所謂 TCP 三向交握，並且是每個使用 TCP 傳輸協定建立連線的基礎。

另一種使用者資料元協定(User Datagram Protocol, UDP 協定)用於簡單訊息傳輸。TCP 是更複雜的協定，因為它的狀態性設計結合了可靠傳輸和資料流服務。協定中其他重要協定有資料擁塞控制協定(datagram congestion control protocol, DCCP)與串流控制傳輸協定(stream control transmission protocol, SCTP)，詳見圖 6 所示。



資料來源：本計畫整理

圖6 傳輸層資料傳輸

●傳輸層包括：

TCP、UDP、DCCP、SCTP、資源預留協定(resource reservation protocol, RSVP)、點對點隧道協定(point to point tunneling protocol, PPTP)、傳輸層安全性協定(Transport Layer Security, TLS)/安全通訊協定(Secure Sockets Layer, SSL)。

2.1.1.5 會議層

會議層(Session Layer)位於 OSI 模型的第 5 層，工作為兩個會議層實體進行對談(Session)管理服務。

會議層為用戶端的應用程式提供開啟、關閉和管理會話機制。對談包含對其

他程式作會話連結的要求及回應其他程式提出的會話連結要求。

2.1.1.6 表現層

表現層(Presentation Layer)主要針對不同終端的用戶提供資料和資訊正確的語法表示變換方法。例如文字檔案的 ASCII 格式與 EBCDIC，用於表示數位的一補數(1's complement)或二補數(2's complement)表示型式。

2.1.1.7 應用層

應用層(Application Layer)是 OSI 模型的第七層，提供為應用軟體的介面，以設定與另一應用軟體之間的通訊，應用層也向第六層表現層發出請求。

- 應用層包括：

超文字傳輸協定(hypertext transfer protocol, HTTP)、超文字傳輸安全協定(hypertext transfer protocol secure, HTTPS)、檔案傳輸協定(file transfer protocol, FTP)、Telnet、安全殼協定(Secure Shell, SSH)、簡易郵件傳輸協定(simple mail transfer protocol, SMTP)、郵件接收協定第 3 版(post office protocol, POP3)等。

2.1.2 TCP/IP 與 DoD 四層模型

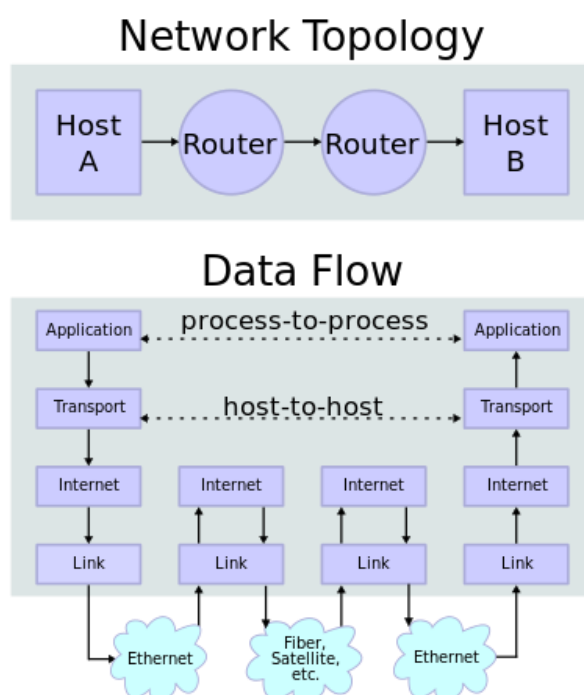
1960 年代，美國國防部（Department of Defense, DoD）為了使資料能夠在眾多不同規格的電腦中互相通訊，於是成立 ARPA（Advanced Research Project Agency）單位，ARPA 架設一個實驗性的網路，稱為 ARPANET。ARPANET 使用一個稱為網路控制程式(Network Control Protocol, NCP)的通訊協定。

1970 年代，ARPANET 由實驗性網路改為運作式網路，ARPA 單位亦改名為國防高等研究計畫署(Defense Advanced Research Projects Agency, DARPA)，此時 DARPA 逐漸將 NCP 通信協定改換成 TCP/IP 的模式，惟

仍是 TCP/IP 的雛型。

1980 年代，DARPA 以低價提供各界測試使用，一直到加州柏克萊大學將 TCP/IP 植入 BSD Unix，TCP/IP 才正式問世。

TCP/IP 提供點對點的連結機制，是目前廣泛被應用的網路協定，它將資料的封裝、定址、傳輸、路由清楚定義，包含資料在目的地如何接收都予以標準化。它將軟體通訊過程簡化為四層，採取協定堆疊的方式，分別實作出不同通訊協定。協定群組下的各類協定，依其功能屬性作用不同，被分別歸屬到這四個階層之中，常被視為是簡化的七層 OSI 模型，詳見圖 7 所示。



資料來源：本計畫整理

圖7 路由器間對應的層連線

TCP/IP 的蓬勃發展發生在 1990 年代中期，當時一些重要而可靠的工具的誕生，例如網頁描述語言 HTML 和瀏覽器 Mosaic，促成網際網路應用的快速發展。隨著網際網路的發展，目前流行的 IPv4 協定已經接近它的功能上

限。IPv4 最致命的兩個缺陷在於：

- 位址只有 32 位元，IP 位址空間有限。
- 不支援服務品質優化控制(Quality of Service, QoS)的想法，無法管理頻寬和優先順序，不能充分支援越來越多即時的語音和視訊應用，因此出現 IPv6 用以取代 IPv4。

TCP/IP 成功的原因在於對眾多的底層協定的支援，這些底層協定對應 OSI 模型中的第一層(實體層)和第二層(資料連結層)。每層的所有協定幾乎都有一半數量支援 TCP/IP，例如：乙太網路(Ethernet)、環狀網路(Token Ring)、FDDI、PPP、X.25、訊框中繼(Frame Relay)、ATM、同步光纖網路(Synchronous Optical Networking, Sonet)、同步數位階層(Synchronous Digital Hierarchy, SDH)等。

整個通訊網路可以劃分成不同的功能區塊，就是所謂的層級(layer)。用於網際網路的協定可以比照 TCP/IP 參考模型進行分類，TCP/IP 協定起始於第三層協定 IP(網際協定)。所有這些協定都在相應的 RFC 文件中討論及標準化，重要的協定在相應的 RFC 文件中均標記狀態：「必須」(required)，「推薦」(recommended)，「可選」(selective)，其他的協定還可能有「試驗」(experimental)或「歷史」(historic)的狀態。

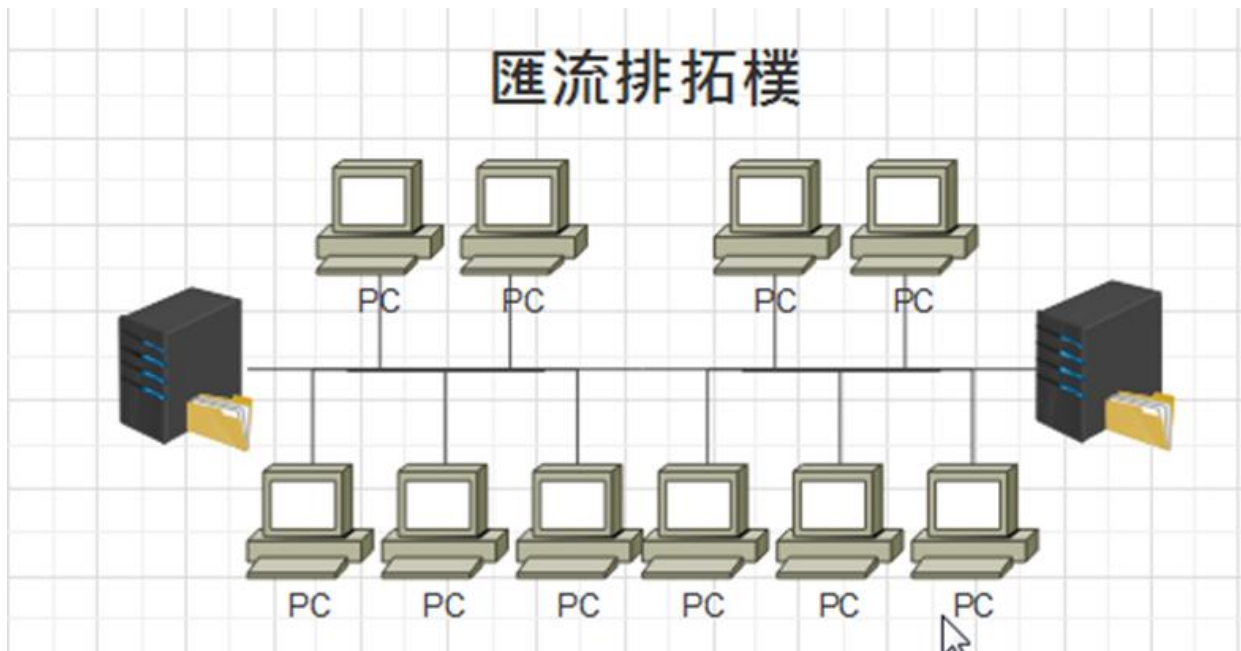
所有的 TCP/IP 應用都必須實現 IP 和 ICMP，以路由器(router)而言，需要有這兩個協定協助做最基本的運作。實際的路由器一般還需要執行許多「推薦」使用的協定，以及一些其他的協定，才能夠正常完整的運作，如圖 7 路由器間對應的層連線。目前 IPv4 協定廣泛運用在網際網路上的電腦，IPv4 協定誕生在 1981 年，目前的版本和初期版本並無多少改變。升級版 IPv6 的誕生於 1995 年，主要目的在於取代 IPv4 的缺點，目前台灣也已經廣泛運用於各種場域中。ICMP 協定主要用於收集網路的資訊尋找錯誤等工作。

2.1.3 網路拓樸型態

網路拓樸係指構成網路的元件間特定的排列方式，區分為實體性或者邏輯性，亦稱之為真實性及虛擬性兩種。如果兩個網路的連接結構相同，儘管它們各自內部的實體接線方式、節點間距離可能會有不同，我們仍就稱它們的網路拓樸相同，常見的網路拓樸型態，摘述如後：

2.1.3.1 匯流排拓樸(Bus)

匯流排拓樸以一條同軸電纜來連接所有的節點，線路二端末處需以終端電阻來結束，匯流排網路中的任一節點都可以傳送訊息至另一個節點中，新增或刪除某一節點也不會影響到網路上的其他電腦，但是當網路資料流量大時，會比星狀或環狀網路更容易產生信號碰撞(Collision)的問題，故二個節點之間需要保持一定之間隔，且當線路中斷時，則同一迴路中的所有電腦將無法通連。常用於早期的乙太網路，現已被星狀或樹狀拓樸結構所取代，匯流排狀網路拓樸示意，詳見圖 8 所示。



資料來源：本計畫整理

圖8 匯流排拓樸架構

●優點

- 較少的電纜長度、適合用於小型網路。

●缺點

- 主纜中斷時，整個網路也將跟著中斷。
- 終端機必須於主幹電纜的兩端。
- 如果整個網路發生中斷時，將會很難找出問題。

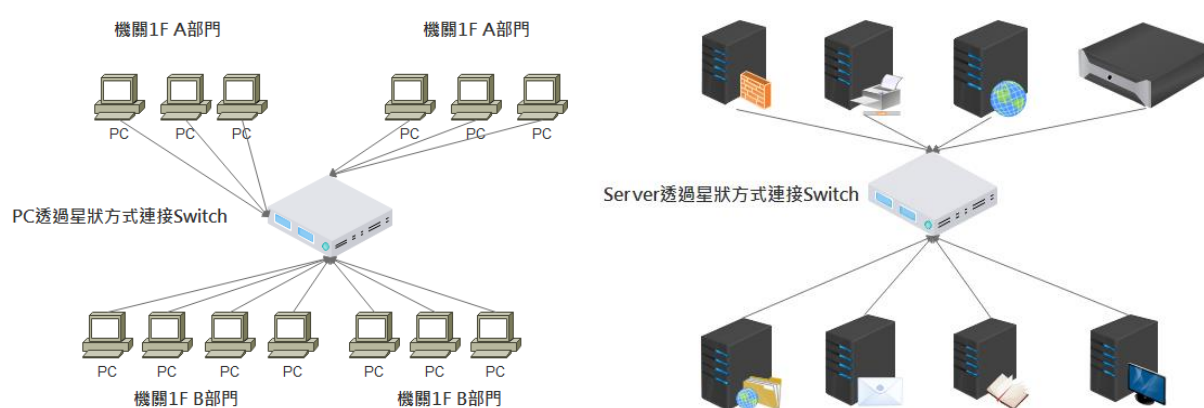
2.1.3.2 星狀拓樸(Star)

星狀拓樸利用一個中央交換中心(Central Switch)來連接網路之活動，端點以點對點方式與交換中心連接。端點間資料傳遞，係透過交換中心以電路交換方式傳送，屬集中式的控制。

它所採用的傳輸介質一般都是採用無遮蔽的雙絞線，端點和中央網路集中設備直接連接，需要耗費較多纜線，安裝維護的工作也較多。

節點擴展時只需要從集線器或交換機等集中設備中拉一條電纜即可，而要移動一個節點只需要把相應節點設備移到新節點即可。

故障診斷和隔離容易，一個節點出現故障不會影響其它節點的連接，惟中央節點的負擔較重，易形成瓶頸，且中央節點一但發生故障，則整個網路都受到影響。星狀網路拓樸示意，詳見圖 9 所示。



資料來源：本計畫整理

圖9 星狀網路架構圖

●優點

- 網路結構簡單，便於管理、維護。
- 控制簡單，添加或刪除某個節點非常容易。
- 集中管理，方便提供服務和網路重新配置。
- 節點直接連到中央交換中心，容易檢測和隔離故障。

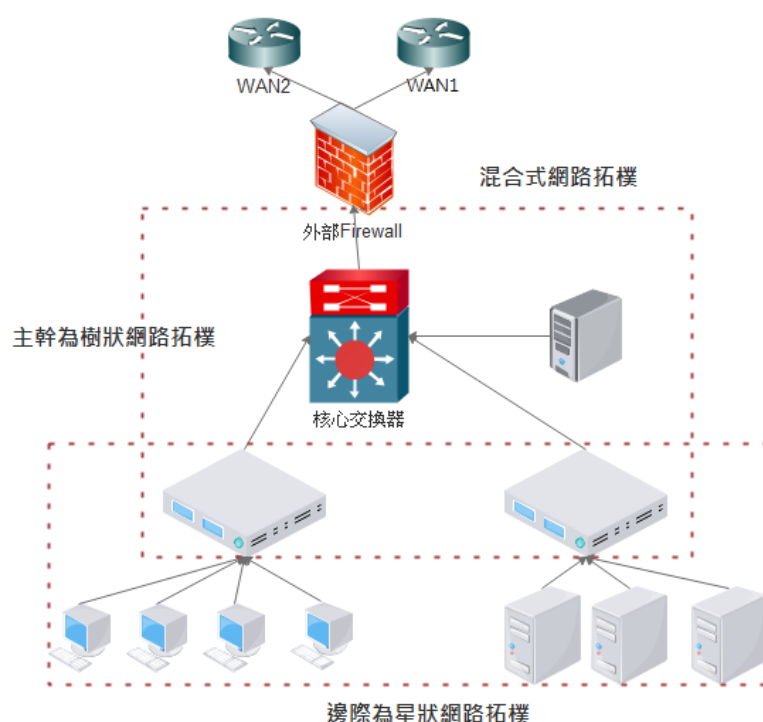
●缺點

- 線路利用率不高，一條線路只被該線路上的一個節點使用。

- 中央交換中心負荷太重，而且當產生故障時，全部網路將無法工作。
- 安裝和維護費用高，需要大量電纜。

2.1.3.3 樹狀拓樸(Tree)

樹狀拓樸是星狀網路拓樸的延伸，利用多分支的傳輸媒體所構成，各端點利用硬體介面直接與傳輸媒體連接。當某一端點傳送資料至傳輸媒體時，各端點均能接收到該資料。單一網段的傳輸距離有限的情形下，便可以利用樹狀拓樸結構，延伸網段之傳輸距離，但是因為每個節點所產生之延遲，故其延伸仍有其極限。例如：舊式的乙太網路架構中，最長延伸距離不可以超過5個網段，新式的網路設備則採用全雙工和交換器(switch)技術下，已經能克服網路信號碰撞的問題。樹狀拓樸架構示意圖，詳見圖10所示。



資料來源：本計畫整理

圖10 樹狀網路架構圖

●優點

－ 通信線路長度短，成本較低，節點易於擴充，尋找路徑比較方便。

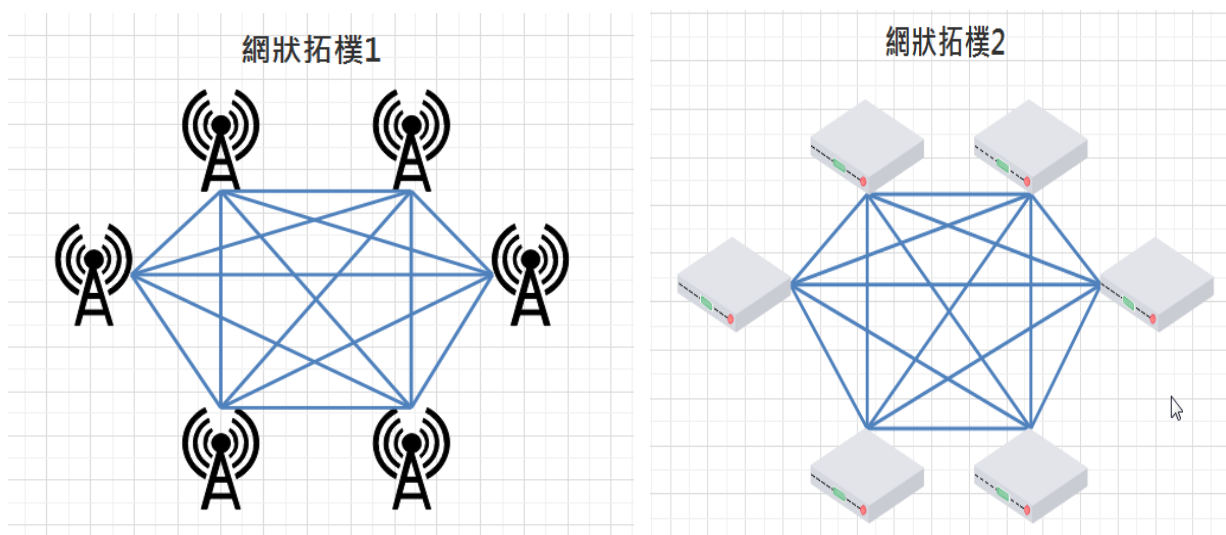
●缺點

－ 節點或其相連的線路故障都會使系統受到影響。

2.1.3.4 網狀拓樸(Mesh)

網狀拓樸是一種在網路節點間透過動態路由的方式，來進行資料與控制指令的傳送，這種網路可以保持節點間連線完整，當網路拓樸中有某節點失效或無法服務時，這種架構允許使用「跳躍」的方式形成新的路由後將訊息送達傳輸目的地。

在網狀拓樸中，所有節點都可與拓樸中所有節點進行連線而形成一個「廣域網路」，網狀拓樸具自我調校機制，即使在拓樸中有節點無法服務或過於忙碌，網路還是可以正常運作。因而形成一個高度可信賴的網路架構。這種架構適用於廣域網路。網狀拓樸架構示意圖，詳見圖 11 所示。



資料來源：本計畫整理

圖11 網狀拓樸架構

●優點

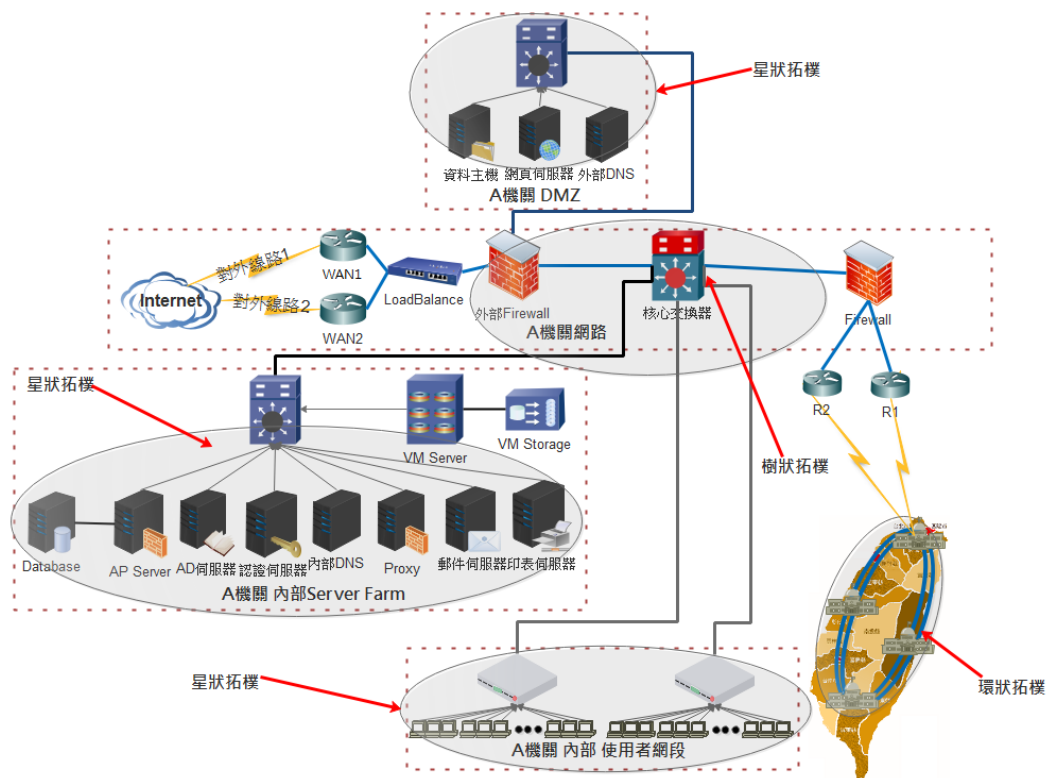
－系統可靠性高，容錯能力優。

●缺點

－費用高，安裝也複雜，管理難度高。

2.1.3.5 混合式拓樸(Hybrid)

使用任何兩種或多種網路拓樸結構之組合，以這種方式，所得到的網路呈現不同標準的拓樸結構(例如：樹狀、星狀、環狀等拓樸)中的一個。舉例來說，一個樹狀網路連接到另一樹狀網路仍然是一個樹狀網路拓樸，而混合式拓樸是產生兩種以上不同的基本的網路拓樸結構所連接，混合式拓樸示意，詳見圖 12 所示。



資料來源：本計畫整理

圖12 混合式拓樸架構

●優點

- 可擴展性：容易透過添加新的組件，增加網路的規模。
- 靈活性佳：混合網路可以根據組織的要求來設計。

●缺點

- 設計複雜。
- 成本昂貴。

2.1.4 軟體定義網路

可程式網路的概念與其後提出的軟體定義網路(Software-defined networking, SDN)大幅地降低了網路維護、管理與更新的困難度，使得網管人員能夠以高階(軟體)的方式取代傳統低階(硬體)的方式調整網路的決策。近來，Google 與許多學術及商業機構已經或投入研發或更新系統為 SDN 架構，顯示它降低維護與營運成本的潛力。

2.1.5 網路功能虛擬化(NFV)

另一個經常跟 SDN 相提並論的技術是網路功能虛擬化(Network functions virtualization, NFV)，近年也受到相當熱烈的關注，但兩者之間其實有所不同。

對於設計、部署、管理網路服務的需求，NFV 提供新的作法。它的主要訴求跟 SDN 有些類似，但面向不同，NFV 可解除眾多網路功能與硬體設備之間的耦合關係。例如將網路位址轉換(Network Address Translation, NAT)、防火牆、網路入侵偵測系統(Intrusion-detection system, IDS)、網路入侵系統防禦系統(Intrusion Prevention System, IPS)、網路入侵偵測 / 防禦系統(IDS/IPS, IDP)、網域名稱服務(domain name system, DNS)、網站快取等網路功能，從專屬的硬體設備當中脫離，讓它們可以在軟體中執行。

設計上，NFV 是用來整併網路元件，並且能將這些網路元件的功能提供出

去，以支援虛擬化基礎架構，包含受到虛擬化的伺服器、儲存，甚至網路，當中運用標準的 IT 虛擬化技術，能執行在高容量的伺服器、交換器與儲存硬體設備，以便虛擬化網路相關的功能。對任何資料層的處理或控制層的功能來說，不論是用在有線或無線網路環境，NFV 都可適用。

2.2 運作原理

2.2.1 乙太網路

乙太網路是一種區域網路技術，IEEE 組織的 IEEE 802.3 標準制定乙太網路的技術標準，內容規定實體層連線、電子訊號和傳輸介質存取層協定的內容，乙太網路是目前應用最普遍的區域網路技術。

乙太網路的原始拓樸結構為匯流排型拓樸，乙太網路為了減少封包傳輸衝突，提高網路速度和最大化使用效率，使用交換器來進行網路封包連線處理與端點連接。透過交換器的連接，乙太網路拓樸結構轉換成星型拓樸，但在邏輯上乙太網路仍然使用匯流排型拓樸和載波多重存取/碰撞偵測 (Carrier Sense Multiple Access/Collision Detection, CSMA/CD) 的匯流排技術。乙太網路交換器主要是要解決封包碰撞與重送的問題，透過將橋接功能用硬體架構實現，藉此能保證轉發資料速率能達到需求。

目前乙太網路都是使用交換器代替集線器(Hub)，兩者佈線方式相同，但交換式乙太網路比集線式(Hub)乙太網路有很多明顯的優勢，例如更大的頻寬和更好的異常結果隔離處理機制。交換器運作時，一開始也和 Hub 一樣，轉發所有資料到所有埠(port)。不同的是當它記錄每個埠的位址後，就只把非廣播資料傳送給特定的目的埠。因此實際速度在任何埠對之間傳送，所有埠對之間的通訊互不干擾。

因為封包一般只是傳送到他的目的埠，所以交換式乙太網路上的流量要小於集線式乙太網路。但交換式乙太網路仍然是不安全的網路技術，很容易因

為 ARP 欺騙攻擊或者 MAC 滿溢攻擊而癱瘓，同時網路管理者也可以利用監控功能抓取網路封包分析，造成資安上的漏洞。

2.2.1.1 早期的乙太網路

10Mbps 乙太網路、10BASE-T 電纜、10BASE5、10BASE-T 、100Mbps 乙太網路。

2.2.1.2 快速乙太網路

- Fast Ethernet 為 IEEE 在 1995 年發表的網路標準，能提供達 100Mbps 的傳輸速度。
- 100BASE-T、100BASE-FX。
- 1Gbps 乙太網路。
- 1000BASE-T、1000BASE-SX、1000BASE-LX、1000BASE-LHX、1000BASE-ZX。

2.2.1.3 10Gbps 乙太網路

10G 乙太網路標準包含 7 種不同類型，分別適用於區域網路、都會網路和廣域網路。目前使用附加標準 IEEE 802.3ae，將來會合併進 IEEE 802.3 標準。

- 10GBASE-SR：用於短距離多模光纖，根據電纜類型能達到 26-82 公尺，使用新型 2GHz 多模光纖可以達到 300 公尺。
- 10GBASE-LR 和 10GBASE-ER：透過單模光纖分別支援 10 公里和 40 公里
- 10GBASE-T：使用遮蔽或無遮蔽雙絞線，使用 CAT-6A 類線至少支援 100 公尺傳輸。CAT-6 類線也在較短的距離上支援 10GBASE-T。

2.2.1.4 40G/100Gbps 乙太網路

新的 40G/100G 乙太網路標準在 2010 年中制定完成，包含若干種不同的節制類型，目前使用附加標準 IEEE 802.3ba。

- 40GBASE-KR4：背板方案，最少距離 1 公尺。
- 40GBASE-CR4 / 100GBASE-CR10：短距離銅纜方案，最大長度大約 7 公尺。
- 40GBASE-SR4 / 100GBASE-SR10：用於短距離多模光纖，長度至少在 100 公尺以上。
- 40GBASE-LR4 / 100GBASE-LR10：使用單模光纖，距離超過 10 公里。
- 100GBASE-ER4：使用單模光纖，距離超過 40 公里。

2.2.2 光纖網路

2.2.2.1 光纖網路技術種類

光纖網路(Fibre Channel，簡稱 FC)是一種高速網路傳輸技術(通常的運行速率有 2Gbps、4Gbps、8Gbps 和 16Gbps)，主要用於連接網路儲存設備。另一種新的乙太網路光纖網路通道標準(Fibre Channel over Ethernet, FCoE)，它利用乙太網路，傳送光纖網路(Fibre Channel)的訊框，讓光纖通信的資料可以在 10 Gigabit 乙太網路骨幹中傳輸，但仍然是使用光纖網路的協定。

2.2.2.2 光纖網路協定說明

FC 協定是完全獨立的網路協定，相較乙太網路較為複雜。FC 自 1988 年出現以來，已經發展成複雜、高速的網路技術。Fibre Channel 可以稱為 FC 協定或者 FC 網路，像 TCP/IP 一樣，FC 協定集同樣具備 TCP/IP 協定集以及乙太網路中的很多概念，比如 FC 交換、FC 交換機、FC 路由、最短路徑優

先(Open Shortest Path First, SPF)路由演算法等。

2.2.2.3 Fibre Channel 特性說明

FC 協定只是定義一套完整的網路傳輸體系，並沒有定義例如小型電腦系統介面(SCSI，Small Computer System Interface, SCSI)或高技術配置(Advanced Technology Attachment, ATA)指令集這樣可用於向磁碟存取數據的通用語言。

FC 是一個高速高效、設定簡單、不需要太多人為設定的網路，基於這個原則，為了進一步提高 FC 網路的速度和效率，在 FC 終端設備上，FC 協定的大部分邏輯被直接設計到一塊獨立的硬體卡片中，而不是運行在作業系統中。

2.2.2.4 Fibre Channel 與乙太網路的比較

TCP/IP 就是一種運行於主機作業系統上的網路協定，其 IP 和 TCP 或 UDP 模塊是運行在作業系統上的，只有乙太網路邏輯部分是運行在乙太網卡晶片中，CPU 從乙太網卡接受到的數據是攜帶有 IP 表頭及 TCP/UDP 表頭，需要運行在 CPU 中的 TCP/IP 協定代碼來進一步處理這些表頭，才能生成最終的應用程式需要的數據。

而 FC 協定的實體層到傳輸層的邏輯，大部分運行在 FC 相容硬體的晶片中，只有小部分關於上層 API 的邏輯運行與作業系統 FC 卡驅動程序中，這樣就使 FC 協定的速度和效率都較 TCP/IP 協定高。但相對而言也增加維運成本，所以 FC 網路並非是針對一般使用設計，多數會運用於高速存取的資料儲存設備網路中，透過增加成本來提高速度和效率。

2.2.3 路由協定

路由協定(Routing Protocol)是一種指定封包轉送方式的網路協定，路由器通過路由表來轉發或接收資料，轉發策略可以是人工指定(通過靜態路由、策

略路由等方法)，一般在較小規模的網路中，比較常使用人工指定策略。

但在較大規模的網路中(如跨國企業網路、ISP 網路)，較少使用人工指定轉發策略，主要是因為避免造成網路管理員管理、維護路由表的困難。

為了處理大型或複雜網路上的路由，動態路由協定應運而生，動態路由協定可以讓路由器自動學習到其他路由器的網路，當網路拓撲發生改變後會自動更新路由表，網路管理員只需要配置動態路由協定即可，相比人工指定策略，在管理與時效及彈性上都有優勢。

2.2.3.1 RIP

路由資訊協定(Route Information Protocol, RIP)很早就被用在 Internet 上，是最簡單的路由協定，主要傳遞路由資訊，通過每隔 30 秒廣播一次路由表，維護相鄰路由器的位置關係，同時根據收到的路由表資訊計算自己的路由表資訊。RIP 是一個距離向量路由協定，最大 hop 數為 15，超過 15hop 的網路則認為目標網路不可到達。此協定通常用在網路架構較為簡單的小型網路環境。現在分為 RIPv1 和 RIPv2 兩個版本，後者支援 VLSM 技術以及一系列技術上的改進。相對其它動態路由 RIP 的收斂速度較慢，但設定也相對簡單。

2.2.3.2 OSPF

開放式最短路徑優先(Open Shortest Path First, OSPF)協定屬於鏈路狀態路由協定。OSPF 提出「區域(area)」的概念，每個區域中所有路由器都有著一個相同的網路狀態資料庫(LSDB)。區域又分為骨幹區域(骨幹區域的編號必須為 0)和非骨幹區域(非 0 編號區域)，如果一個運作的 OSPF 的網路只存在單一區域，則該區域可以是骨幹區域或者非骨幹區域。如果該網路存在多個區域，那麼必須存在骨幹區域，並且所有非骨幹區域必須和骨幹區域直接相連。

OSPF 利用所維護的網路狀態資料庫，通過最短路徑優先演算法(SPF 演算

法)計算得到路由表，OSPF 的收斂速度較快。由於其特有的開放性以及良好的擴充功能，目前 OSPF 協定在各種網路中是最為廣泛使用動態路由協定。

2.2.3.3 IS-IS

中間系統到中間系統協定(Intermediate system to intermediate system, IS-IS)屬於網路狀態路由協定，標準 IS-IS 協定是由國際標準化組織制定的 ISO/IEC 10589:2002 所定義，標準 IS-IS 不適合用於 IP 網路，因此 IETF 制定適用於 IP 網路的整合化 IS-IS 協定(Integrated IS-IS)。

與 OSPF 相同 IS-IS 亦使用「區域」的概念，同樣也維護著一份網路狀態資料庫，通過最短路徑優先演算法(SPF)計算出最佳路徑。IS-IS 的收斂速度較快，整合化 IS-IS 協定是 ISP 骨幹網上最常用的 IGP 協定。

2.2.3.4 IGRP

企業網路閘道路由協定(Interior Gateway Routing Protocol, IGRP)由 Cisco 於 1980 年代獨立開發，屬於 Cisco 私有協定。IGRP 和 RIP 一樣，同屬距離向量路由協定，因此在諸多方面有著相似點，如 IGRP 也是周期性的廣播路由表，也存在最大 hop 數(預設為 100，達到或超過 100 hop 則認為目標網路不可達)。

IGRP 最大的特點是使用混合度量值，同時考慮網路的頻寬、延遲、負載、最大傳輸單元(Maximum Transmission Unit, MTU)、可靠性等 5 個方面來計算路由的度量值，而不像其他內部閘道協定(Interior Gateway Protocol, IGP)協定單純的考慮某一個方面來計算度量值。

目前 IGRP 已經被 Cisco 獨立開發的加強型閘道間選徑協定(Enhanced Interior Gateway Routing Protocol, EIGRP)協定所取代，因此 Cisco IOS(Internet Operating System)v.12.3 及其以上的已不支援 IGRP 協定，現在已經罕有執行 IGRP 協定的網路。

2.2.3.5 EIGRP

由於 IGRP 協定的種種缺陷及不足，Cisco 開發 EIGRP 協定來取代 IGRP 協定。EIGRP 屬於高階距離向量路由協定(又稱為混合型路由協定)，繼承 IGRP 的混合度量值，最大特點在於引入非等價負載均衡技術，並擁有極快的收斂速度，EIGRP 協定在 Cisco 裝置網路環境中廣泛部署。

2.2.3.6 BGP

為維護各個 ISP 的獨立運作，標準化組織制定 ISP 間的路由協定 BGP。BGP 是「邊界閘道器協定(Border Gateway Protocol)」的縮寫，處理各 ISP 之間的路由傳遞。但是 BGP 執行在相對核心的地位，需要用戶對網路的結構有相當的了解，否則可能會造成設定錯誤與衍生的損失，一般網路中不會使用到 BGP 協定。

2.2.4 網路管理協定

網路常見的網路管理協定茲以下列 3 種，摘述如后：

2.2.4.1 簡單網路管理協定(SNMP)

2.2.4.1.1 協定說明

簡單網路管理協定(Simple Network Management Protocol, SNMP)是 IETF 所定義的 Internet 協定一部分，協定能夠支援網路管理系統，主要用以監測連線到網路上的裝置是否有任何引起管理上需要關注的情況，內容由一組網路管理的標準組成，包含應用層協定(Application Layer Protocol)、資料庫模型(Database Schema)和資料內容。

2.2.4.1.2 運作說明

SNMP 主要分為管理端(Manager)、代理者(Agent)以及網路管理資料庫(Management Information Base, MIB)三個元件，分述如後：

●管理端

管理端(Manager)通常被稱為網路管理工作站(Network Management Station, NMS)。利用 SNMP 通訊協定向代理者(Agent)查詢所需的相關資訊，如網路設備運作狀態、系統硬體的配置(如 CPU 使用率、硬碟利用率)等。

管理者取得此類資訊後，即可進行統計分析，並且利用相關工具進行處理，繪出簡單易懂的統計圖表供使用者瀏覽。

SNMP 定義 Manager 與 Agent 的溝通指令，詳見圖 13 所示。

	指令	說明
1	Get Request (讀取請求)	由管理端發給代理者，用來讀取代理者所取得的數值，如設備狀況等。
2	Get Next Request (讀取下一個請求)	由管理端發給代理者，讀取下一個物件，由於 SNMP 限定管理端一次僅能取讀一個資訊，因此只能用此指令取得下一個物件資訊。
3	Get Respond (讀取回應)	取得不同指令的回應值，如果指令順利執行成功，即取得相關的數據，如果指令執行失敗，也可取得錯誤訊息。
4	Set Request (設置請求)	用來設定代理者上某個物件的值。
5	Trap (異常狀況)	當代理者所設定的異常狀況發生時(如設備重啟)，即由代理者單向告知給管理端，用來報告異常狀況。

資料來源：本計畫整理

圖13 SNMP Manager 與 Agent 的溝通指令

●代理者

代理者通常是一個執行程式(通常運作在被監控的設備上)，負責讀取被監控設備上的相關資訊，而後接收到管理端所發出的 SNMP Get-request、Get-next-request 等查詢指令時，再將相關資訊回傳至管理端。

除了資料回傳的機制外，代理者也提供主動回報的機制(Trap)，在符合條件的情況下(如系統發生錯誤或關機等特殊的情況)主動地以 Trap 的方式發送訊息通知管理端。

●網路管理資料庫

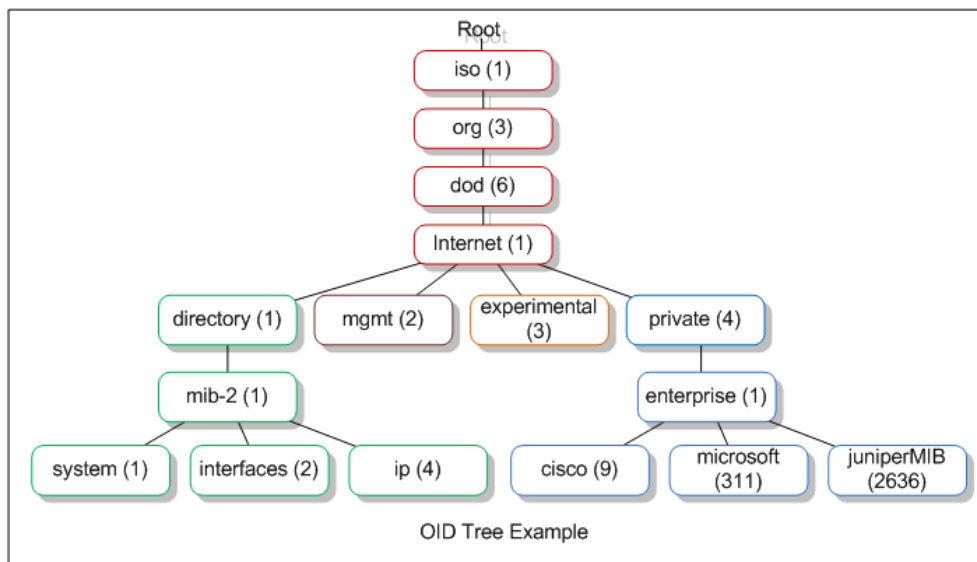
由於 SNMP 通訊協定的原始要求，在於適用各種類型的網路設備，所以它所管理的資訊亦隨著網路設備的種類而有所不同。

但在現實環境中，每種網路或設備對其資料的表達方式也存在大小不一的差異，因此必須採用一套抽象的語法來描述所有類型的資訊。

因此 SNMP 定義 MIB，利用階層性的描述，說明所有受管理設備資訊的屬性，並將這些設備稱為 SNMP 物(Object)。

MIB 可分為標準(Standard)MIB 及私人(Private)MIB 兩大類，標準 MIB 適用於所有網路設備，而 Private MIB 則由設備廠商自行定義，以反映該設備獨特的數值(如各家廠商標榜獨特的功能)。合法的私人 MIB 就跟網址一樣，需要向有關單位申請，以確保每一個 Private MIB 都是全球獨一無二的。

MIB 採用樹狀結構，是一種階層式分類。其中每個節點皆有自己特定的類型，以易於人類辨識的單字標記，並附有物件身分編號，亦即物件識別碼(Object Identifier, OID)，而樹狀末端的所有葉片為 SNMP 定義的物件。詳見圖 14 所示。



資料來源：本計畫整理

圖14 管理資訊庫的樹狀結構圖

上圖中，樹狀結構內的物件均會分配一組唯一的物件識別碼(OID)，如上述結構中的 internet，物件識別碼表示方法即為 iso.org.dod.internet 或 1.3.6.1，SNMP 即可利用物件識別碼資訊來識別被監控設備，並用來取得被監控設備的狀態，或者，利用設定物件識別碼資訊來設定被監控設備的狀態。

2.2.4.1.3 SNMP 各版本說明

隨著時代的演進，SNMP 版本也不斷地更新，以符合環境現狀所需。目前 SNMP 版本分為 SNMP v1、SNMP v2、SNMP v3，以下簡略說明這三個版本的差異性。

●SNMP v1 主要存在的問題：

僅定義管理端對代理者的關係，並沒有定義管理者對管理者的關係，因此在一個網路環境中僅能部署一個管理系統，不適用於大型的網路環境。

無法一次傳送大量的資料，因此必須花費較多的時間重複地下達命令，

方可取得相關的資料。

僅提供簡單的身分認證機制(僅利用 community 名稱來控管)，在安全性上具有相當大的疑慮。

採用 Pooling(輪詢)的管理方式，如果間隔時間過長，則會有無法即時取得代理者相關資訊的情況，但設定間隔時間如果過短，大量的傳輸封包又會影響網路的使用效能。

- 由於 SNMP v1 有上述的缺點，因而又提出 SNMP v2 通訊協定，主要改良的地方說明如後：

新增 getbulkrequest 命令，讓管理端只要下達一次命令即可取得大量相關資料，而不必藉由多次的存取來取得相關資料，可有效增進網路使用的效能。

新增 informRequest 指令，增強管理端與管理端的溝通能力，讓彼此間能夠互相交換訊息。擺脫 SNMP v1 一個網路環境只能部署一個管理系統的缺點，有利於大型網路環境管理。

- SNMP 第三版由 RFC 3411-RFC 3418 定義，主要增加 SNMP 在安全性和遠端配置方面的強化，SNMP 第三版提供重要的安全性功能，包含資訊完整性，檢驗資訊來自正確的來源，封包加密。

2.2.4.2 NetFlow

2.2.4.2.1 協定說明

NetFlow 是一種網路監測功能，可以收集進入及離開網路界面的 IP 封包的數量及資訊，最早由思科公司研發，應用在路由器及交換器等產品上。

Cisco 的 NetFlow 也有多種版本，如 V5、V7、V8、V9，目前 NetFlow V5 是主流。

2.2.4.2.2 運作說明

以 NetFlow V5 說明，一個 IP 數據封包的 Flow 至少定義 7 個主要項目：

- 來源 IP 位址
- 目的 IP 位址
- 來源埠號
- 目的埠號
- 第三層協定的類型
- TOS(Type of Service)欄位
- 網路設備輸入/輸出的邏輯埠(if index)

以上 7 個欄位定義一個基本的 Flow 訊息，NetFlow 就是利用分析 IP 網路封包中的上述 7 種屬性，快速區分網路中傳送的各種類型的實際網路數據流量。

2.2.4.2.3 Cache 管理

在 NetFlow Cache 管理中有兩個主要組件：

- NetFlow Cache

主要描述來源封包數據如何存放在 Cache 中，NetFlow 暫存管理機制中包含一系列高度精細化算法，能夠有效地判斷一個內容是屬於已存在 Flow 的一部分還是應該在暫存中產生一條新的 Flow。這些算法也能動態更新暫存中 Flow 的資訊，並且判斷哪些 Flow 應該到期終止。

- NetFlow Export

NetFlow Export 為數據封包的輸出機制，主要描述數據封包如何輸出並被

分析器接收。

當 NetFlow Cache(暫存機制)暫存中的 Flow 到期後，就會產生一個將 Flow 輸出的動作。將超時的 Flow 資訊以數據資料的方式輸出，叫做「NetFlow Export」，這些輸出的資料包含 30 條以上的 Flow 資訊。這些 NetFlow 訊息一般是無法識別的，需由專用收集器(Flow Collector)收集到並做出進一步分析，這些 Flow Collector 能夠識別 NetFlow 的特殊格式。

2.2.4.2.4 輸出格式

NetFlow 的輸出資料包含表頭和一系列的 Flow 內容，表頭包含系列號、記錄數、系統時間等，Flow 內容包含具體內容，包含 IP 位址、埠號、路由資訊等。各個版本的 NetFlow 格式都相同，且 NetFlow 採用 UDP 報文，這更有利於大流量情況下的數據報文傳輸。換句話說，在路由器、防火牆等網路設備中如要使用 NetFlow 就不能禁用 UDP 埠，否則無法接收設備傳遞的資訊。

2.2.4.2.5 抽樣機制

在 NetFlow 的實際應用中，不是隨時都把數據封包抓取過來，而是採用抽樣的機制，通過使用抽樣技術可以降低路由器的 CPU 利用率，減少 Flow 的輸出量，但仍然可以監測到大多數的流量訊息。多數情況下不需要了解網路流量的每個 Flow 的具體細節，抽樣是比較好的選擇。採用 NetFlow 計算實際網路流量時會有誤差，輸出並不能準確反映流量的實際情況。

另外實際使用時也需要注意效能損耗的問題，一般僅有高階的 Cisco 設備支援此功能(如 6500、7600 系列等)，設備一般都是通過 ASIC 硬體處理數據封包，但仍會占用 10%~20% CPU 利用率。因此在高網路負載情況下，使用 NetFlow 功能需特別注意。

另外例如當網路不正常運行時也可以透過 Netflow 禁行輔助分析。如因病毒

具有掃描網路，主動傳播病毒的能力，會大量占用網路頻寬或網路設備系統資源。這些蠕蟲在網路行為上都有某些共同特徵，我們可以利用 NetFlow 的訊息篩選出這些封包，從而快速發現問題。

2.2.4.3 sFlow

2.2.4.3.1 sFlow 協定說明

流量採樣協定(Sampled Flow, sFlow)，是一種工業規格，用來測量 OSI 模型第二層封包。這個規格提供了一個方法，以取樣的方式，獲得網路封包的資訊，讓網路管理人員可以了解網路的運作狀況與網路壅塞的原因。

2.2.4.3.2 運作說明

sFlow 和 NetFlow 聽起來很相似，但實際上卻是不一樣。NetFlow 會針對所有流經的網路封包去取得其特徵，包含 Source IP address、Destination IP address、Source port for UDP or TCP、Destination port for UDP or TCP，type and code for ICMP、IP protocol、Ingress interface(SNMP ifIndex)、IP Type of Service 這些資訊。

由於 NetFlow 會對所有流經的封包進行處理，若網路流量極大時，NetFlow 所提供的資料量亦會隨之增加，若資料量太大，後端分析引擎可能會不堪負荷，進而影響資料判讀時的正確性。

2.2.4.3.3 差異性

sFlow 的作法和 NetFlow 不同，sFlow 以取樣的方式取出資料的摘要，使用者可以自訂其取樣大小及取樣週期，經 sFlow 取樣後的資料相對於 NetFlow 而言會大量的減少，如此一來就可以兼顧資料正確性並確保後端分析引擎處理能力。

2.2.5 防火牆運作原理

防火牆最基本的功能就是隔離網路，通過將網路劃分成不同的區域（通常情況下稱為 ZONE），制定出不同區域之間的存取控制策略來控制不同信任程度區域間傳送的資料流。例如網際網路是不可信任的區域，而內部網路是高度信任的區域，以避免安全策略中禁止的一些通訊，它控制資訊基本的任務在不同信任的區域。

防火牆能利用封包的多樣屬性來進行過濾，例如：來源 IP 位址、來源埠號、目的 IP 位址或埠號、服務類型，也能經由通訊協定、TTL 值、來源的網域名稱或網段...等屬性來進行過濾。

防火牆通常亦具有網路網址轉換(NAT) 的功能，將主機保護在防火牆之後使用私有網路位址(Public IP)，定義在 RFC 1918。

2.2.6 OpenFlow 傳輸協定

OpenFlow 是一種軟體定義網路，由開放網路基金會(Open Network Foundation) 所制定一種網路協定，運作於 OSI 七層中的第二層(資料連結層)。這個網路協定主要允許由遠端控制器(Controller)去控制交換機或路由器的資料平面(Data Plane)，動態調整網路封包轉送方式，進而達成集中控管網路設備的目標。

2.2.6.1 OpenFlow 傳輸架構簡介

傳統網路的交換器中，每台網路交換設備(如交換器、路由器等)都包含控制平面(Control Plane)與資料平面(Data Plane)，OpenFlow 協定則是將控制平面自交換設備上分離，並集中由遠端控制器進行管理。因此，交換器僅包含資料平面，並負責與遠端控制器以 OpenFlow 協定以加密/非加密進行溝通，此溝通的通道亦稱為 OpenFlow 通道。傳輸的內容包含控制器至交換器訊息、非同步訊息與對稱訊息。

2.2.6.2 控制器至交換器訊息簡介

控制器至交換器訊息代表著從控制器發送的訊息，根據訊息的內容由交換器選擇回應或不回應。這類訊息包含詢問交換器功能，Flow、Group、Meter 的新增、修改、刪除等功能。

2.2.6.3 非同步訊息簡介

非同步訊息主要是作為主動發送的訊息，而不需要先從另一端發送請求的訊息，這些訊息包含封包到達與發送(Packet in/out)、交換器狀態的改變，以及錯誤訊息。

2.2.6.4 對稱訊息簡介

對稱訊息代表不論是控制器至交換器皆可以發起的訊息，包含建立連線的歡迎訊息、確認對方是否存在的 Echo 訊息，以及實驗訊息。值得一提的是實驗訊息主要是提供給營運商/開發者自定義自己的相關內容，提供 OpenFlow 協定具有各種傳輸訊息對應說明。

2.2.7 NFV 參考架構

NFV 是將原本硬體綁定的功能以軟體方式實現，並定義一系列相關架構，提供給營運商/企業建置在一般商用伺服器的硬體上。在標準制定方面，由歐洲電信標準化協會(以下簡稱 ETSI)為 NFV 制定可擴展的參考架構，並包含五個區塊：虛擬化網路功能區塊(Virtualized Network Function, VNF)、NFV 基礎建設區塊(NFV Infrastructure, NFVI)、NFV 管理與協調流程區塊(NFV Management and Orchestration)、營運與企業支援系統區塊(Operation/Business Support System, OSS/BSS)及服務、虛擬化網路功能及基礎建設描述區塊(Service, VNF and Infrastructure Description)。

2.2.7.1 虛擬化網路功能區塊簡介

虛擬網路功能區塊將原本傳統網路中，將硬體所實現的網路功能虛擬化(VNF)，也就是以軟體的形式來實現，並包含一個以上的功能與網路元件管

理系統(Element Management System, EMS)。一個 EMS 可管理一個至多個 VNF，並搭載在一個至多個虛擬機器上(Virtual Machine)，藉此取代傳統網路的佈建模式，不需要購入各式網路專用硬體。

2.2.7.2 NFV 基礎建設區塊簡介

NFV 基礎建設區塊將硬體與虛擬化的資源進行整合，並提供虛擬化網路功能區塊進行搭載。NFV 基礎建設區塊主要分為虛擬資源(Virtualized Resources)、虛擬層(Virtualization Layer)、硬體資源(Hardware Resources)三個部分。虛擬層介於硬體資源與虛擬資源之間，跨軟硬體整合硬體資源，並將資源虛擬化之後轉化為可即時調度的虛擬資源。

2.2.7.3 NFV 管理與協調流程區塊簡介

NFV 管理與協調流程區塊負責協調流程、管理、驗證與授權相關虛擬化資源的請求，並調整相關 VNF 的啟動、終止、調整虛擬化資源、更新等議題。除此之外，此區塊也負責效能、關聯事件的收集與轉送等。

2.2.7.4 營運/企業支援系統區塊簡介

營運/企業支援系統區塊主要由各營運商或企業導入各自的支援系統與企業支援系統，作為自身計費、業務、營運需求、服務優先等級等相關資料提供。因此，NFV 管理與協調流程區塊在調度相關虛擬化資源時，會參考此區塊所提供的相關優先等級資訊來進行資源配置。

2.2.7.5 服務、虛擬化網路功能及基礎建設描述簡介

主要作為不同營運商/企業在進行跨 NFV 連接時，相互交換的資訊，以提供更恰當的流程及資源管理。服務、虛擬化網路功能及基礎建設描述包含上述區塊相關資訊，如 VNF 部署方法、轉送方式、NFV 基礎建設區塊模型與營運/企業支援系統相關資訊等。

2.3 安全技術

2.3.1 SNMP 安全性

SNMP v2 運用資料加密標準(Data Encryption Standard, DES)與 MD5 等編碼技術對於傳送中的資料進行編碼，以增進網路傳輸時的安全。

SNMP v3 版本即是在 SNMP v2 的基礎上增強安全功能，透過對資料進行鑑別與加密，提供以下幾個的安全特性：

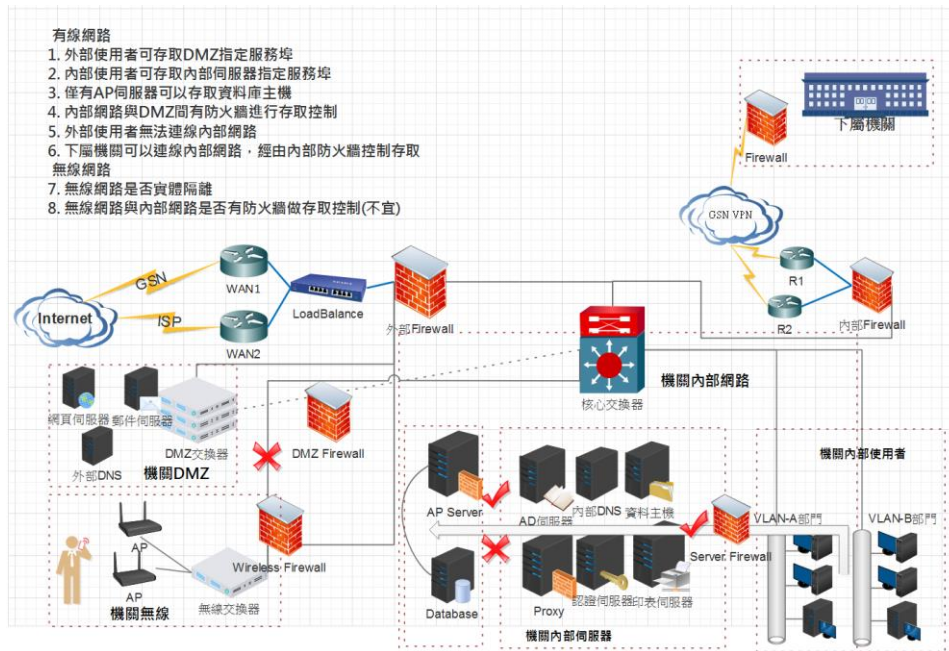
- 確保資料一定是從合法的資料來源發出。
- 對於傳輸的資料進行加密，以確保資料的機密性。
- 利用密碼原理，確保傳輸資料在傳輸過程中不會被篡改。

SNMP v3 的最終目的在於保障管理資訊雙方只接收從合法的資料來源發出，且已被加密並確定未被更改的管理資訊。

SNMP 管理上應注意在可行的狀況下應儘量優先使用 SNMP v3 以確保管理的安全性，若執行上有困難時，可以 SNMP v2 搭配來源限制與唯讀的設定減低管理上的風險。

2.3.2 防火牆安全技術

防火牆(Firewall)是一項協助確保資訊安全的裝置，會依照特定的規則，允許或是限制傳輸的資料通過，防火牆可能是一台專屬的硬體或是架設在一般硬體上的軟體，防火牆最基本的功能就是隔離網路，經由將網路劃分成不同的區域(通常情況下稱為 ZONE)，制定出不同區域之間的 policy 來控制不同信任程度區域間傳送的資料流，達成安全或管理上的需求，詳見圖 15 所示。



資料來源：本計畫整理

圖15 機關網路防火牆樣態

另外目前新型的次世代防火牆相較於以往防火牆強調存取控制外，亦具備URL、網頁內容過濾、IDP、阻斷服務攻擊(denial-of-service attack, DoS)、應用程式控管、頻寬控管等功能。

●應用程式控管

新興應用服務的出現，不僅能提供更多樣化的服務，也讓各種網路資源的取得，有了更便利的途徑。然而，資源唾手可得的同時，網路卻也開始成為惡意攻擊的最佳媒介。應用程式控管可針對常見的應用服務進行管控，如后：

- － 即時訊息工具（IM）：MSN、Yahoo Message、QQ。
- － 點對點下載工具（P2P）：eMule、Bit Torrent、Foxy、迅雷。
- － 社群工具：Facebook、Twitter、Blog。

- 線上影音傳輸：KKBOX、Youtube、PPStream、PPLive、Youku。
- 加密通道工具：無界瀏覽（Ultrasurf）、自由門（Freegate）。
- 線上服務：Google 各種服務、各類 Web mail。

機關應與維護廠商討論管理策略，透過設備內建的特徵碼辨別應用程式，並針對高風險與不合乎機關安全管理機制的程式進行控管或監控，限制其流量。

●URL 內容過濾

針對網頁瀏覽進行 URL 限制，避免機關人員刻意或誤入高風險網站，亦可限制機關人員避免觸及高敏感性的網頁，進而降低因為網頁瀏覽所衍生的風險。

●網頁內容過濾

網頁內容過濾的技術近年已經成熟，各家廠商都會強調網頁分類資料庫的完整性。網頁內容過濾產品會將使用者瀏覽的網頁，與網頁分類資料庫進行比對，以判斷該網頁是否屬於正當內容。網頁分類資料庫內儲存上百萬個網址，大約數十種分類（30~80 餘種），常見的项目包含色情、毒品、賭博、求職、網頁郵件、新聞等。

由於 URL 每天都會不斷的新增與消失，所以資料庫的更新頻率也是選購的重點，大多數產品都強調每日更新。如何更快且更正確的收集 URL，也是廠商努力的重點，有些產品能夠自動回應未分類的網站和應用程式，當使用者瀏覽未知的網站或程式時，系統會將資料回傳原廠，經過人工審核後，該筆資料會在幾天內加入資料庫。

不過，網頁分類資料庫並非萬能，因為它面臨 URL 轉向、多主機位址及未註冊網站等威脅，很容易就失去有效性。為了彌補資料庫的不足，有些

產品增加網頁內容過濾功能，利用關鍵字加權計分等技術，分析 HTML 網頁的內文，如果超過容許值就予以阻擋。

也有廠商認為，網路內容安全不單只是網頁內容過濾而已，還必須執行完整的內容檢查，分析下載的網頁內容和附件。這樣的產品是使用特殊的演算引擎，能夠更完整的分析網頁內容，防止使用者上下載不當的附件。但相對的，它所需的資源和時間也比其他網頁過濾產品來的高。

機關管理時可針對網頁瀏覽或發文中敏感或有問題的內容進行過濾，達到安全控管，或避免觸犯機關的禁令。

●DoS 攻擊防禦

針對 DoS 攻擊進行防禦，需確認此機制是否建置於防火牆，或由單獨設備為之。機關應具備此防禦功能，除確認功能是否具備外，應確認此功能是否正確開啟，若正確開啟，設備每日將偵測到不同等級風險事件。

2.3.3 DNS 安全性設定

2013 年歐洲反垃圾郵件組織 Spamhaus 遭受流量高達 300Gbps 的分散式阻斷服務攻擊(distributed denial-of-service attack, DDoS 攻擊)，進一步探討此次 DDoS 攻擊手法，係採用 DNS 反射/擴大攻擊(DNS reflection/amplification attack)，也就是利用公開的 DNS 解析器(resolvers)，攻擊者假裝從 Spamhaus 對數萬台的 DNS 解析器發出請求，而這些 DNS 解析器會向 Spamhaus 回應，因此帶來大量的網路流量。

理論上，DNS 伺服器應該設定支援來自一個特定的網域名或一個範圍的 IP 位址的請求，不過事實上，全球網路中有高達千萬台的 DNS 伺服器，其初始設定值為對外開放，也就是可以回應來自其支援的網域名以外的需求，因此能被有心人士利用，一但內部目錄管理服務(Active Directory, AD)的 DNS 系統癱瘓，就足以使機關網路近乎停擺。

在 DNS 的安全管理上，建議如後：

- DNS Recursive(DNS 遞迴查詢)

僅允許針對所要服務的網段提供服務。

- Zone Transfer(域名資料傳送)

確認域名資料傳送的存取控制設定，避免讓非法 DNS 任意透過這種方式探詢，以取得組織內的主機資訊。

- Administrator(管理者)

避免系統最高管理權限及單一系統主機，共用相同管理者帳號，以及限制管理者操作權限、限制管理者操作來源位址、落實管理者密碼複雜度等。

- 補強管理資訊與記錄

對於 DNS 攻擊的防護上，相關的網管資訊及事件記錄對於攻擊威脅的預防與應變處理有極大的幫助。

評估 DNS 效能承載時應將網管功能與事件記錄處理狀態考量在內，除了 DNS 主機的處理器、記憶體及網路之外，更應該針對 DNS 各類型的服務狀態與查詢回應記錄，納入監測的管理資訊中，將有助於管理者查覺攻擊發生的異常變化趨勢，以及查找異常網域及 IP 位址來源。

- 提升 DNS 自身防護能力

DNS 的網路服務為了達到低延遲的連線需求，而採用 UDP 協定傳輸，對於偽冒 IP 位址(IP Spoofing)的傳輸行為無法防範，因此如果有人發動相關網路攻擊，例如 DNS 快取下毒(DNS cache poisoning)、透過偽裝 DNS 伺服器發動中間人攻擊(Man-in-the-Middle-attack, MITM)都是很有可能的。

為了解決這項嚴重危害網路安全的問題，2001 年起，IETF 組織開始制定

一套新的標準，稱為 DNSSEC(Domain Name System Security Extensions)。

新一代的 DNS 系統包含 DNS Blacklist、DNSSEC、RRL(Response Rate Limiting)及 RPZ(Response Policy Zones)等，使 DNS 更有能力面對外來的攻擊。

2.3.4 DDoS 防禦技術

DoS 是一種網路攻擊手法，其目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其正常用戶無法存取。

當駭客使用網路上兩個或以上被攻陷的電腦作為「殭屍」，向特定的目標發動「阻斷服務」式攻擊時，稱為 DDoS 攻擊。

面對 DDoS 攻擊，包括機關和 ISP 業者多數無法做到完全的防禦，大部分都從減緩 DDoS 攻擊的強度著手，要做到有效減緩，上游就必須有流量清洗機制，下游則必須要有防禦機制去阻擋。

例如 DDoS 攻擊是從海外的 ISP 業者連進來，已經影響到臺灣像是海纜的頻寬使用，臺灣 ISP 業者可以利用遠端驅動工具，並且呼叫 Tier 1 的 ISP 業者進行聯防，把 DDoS 攻擊在境外阻擋完畢；有些時候，ISP 業者也會利用 Black Hole（黑洞）的機制，把遭受到攻擊的用戶 IP 路由導入黑洞，無法從外部存取到這個網站服務，藉此保全 ISP 業者其他客戶的安全性；如果這些 DDoS 攻擊影響到國內網路安全，ISP 業者也會利用網路存取控制工具搭配邊境管制的手法，阻擋這些 DDoS 攻擊的封包影響臺灣的用戶。

有些時候，DDoS 攻擊太大量時，境外阻絕或邊境控管阻擋不住，還是進到臺灣的網路骨幹，或者是攻擊是來自臺灣內部時，則可以進行骨幹內部的管控，透過限制頻寬的方式，將攻擊封包黑洞或者是把這些封包丟棄。

一旦這些 DDoS 攻擊已經兵臨城下，影響到用戶端的網路服務時，就可以透過 DDoS 隔離清洗的方式，把遭受攻擊的流量導入隔離清洗區，透過網

路設備進行規則式攻擊流量的過濾，並分析一些惡意封包的攻擊行為模式進行阻擋，也可以限制連線數量並作攻擊分析，也可以透過客製化防護等措施，讓攻擊用戶網路服務的流量，可以大部分都被過濾掉，確保用戶網路服務的安全和穩定。

2.3.5 入侵偵測防禦系統

在 OSI 網路模型中，防火牆主要在第二到第四層控制，而入侵防禦系統專門深入網路資料內部，尋找它所認識的攻擊代碼特徵，過濾有害資料，可選擇丟棄並進行記載，以便事後分析。除此之外，入侵防禦系統同時結合考慮應用程式或網路傳輸層的異常情況，來輔助識別入侵和攻擊，用戶或用戶程式違反安全規則時、資料封包在不應該出現的時段出現、操作系統或應用程式弱點的被利用等現象。

入侵偵測防禦系統的目的在於及時識別攻擊程式或有害代碼和變種，採取預防措施，先期阻止入侵，降低危害性。

- 異常偵查

入侵防禦系統知道正常資料及資料之間關係的正常的樣子，可以對照識別異常。

- 動態代碼偵測

入侵偵測系統在碰到動態代碼（ActiveX，JavaApplet，各種指令語言 script languages 等）時，先把它們放在沙盤內，觀察其行為動向，如果發現有可疑情況，則停止傳輸，禁止執行。

- 偵測協定異常、傳輸異常和特徵偵查，對通過閘道器或防火牆進入網路內部的有害代碼過濾並阻止。

- 透過內部資料特徵庫攔截有問題的服務請求，用戶程式通過系統指令享用

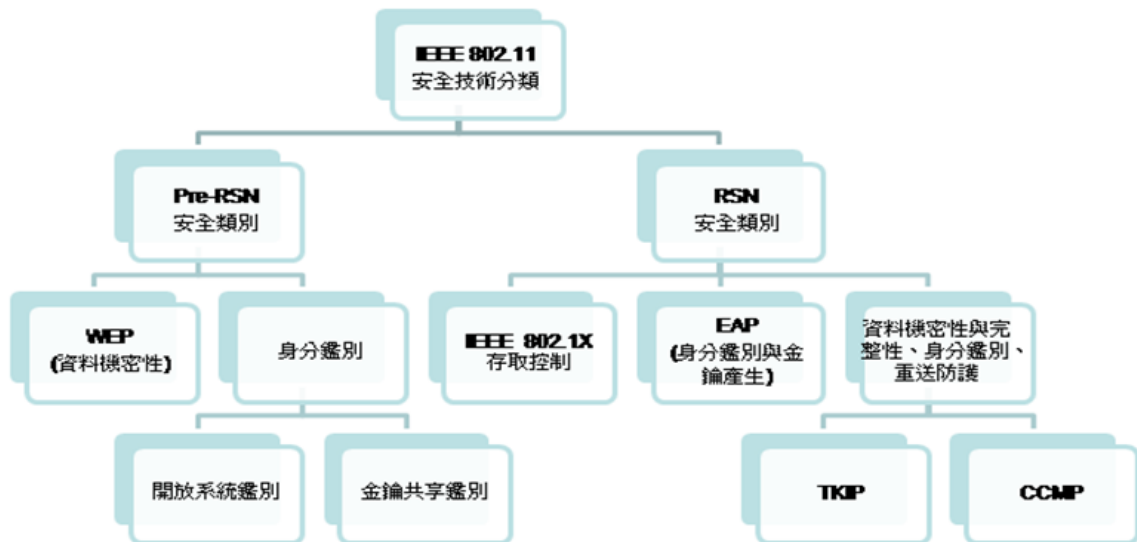
資源（如儲存區、輸入輸出裝置、中央處理器等）。

- 對 Library、Registry、重要檔案和重要的資料夾進行防守和保護。

2.3.6 無線網路安全機制

目前主要之無線網路應用技術包含無線區域網路(IEEE 802.11)與行動通訊(IEEE 802.16、GSM、GPRS、3G、4G、5G、PHS 及衛星系統)等相關技術，這些無線網路傳輸系統的安全技術之範疇皆離不開身分鑑別、存取控制及資料加密等三大機制。

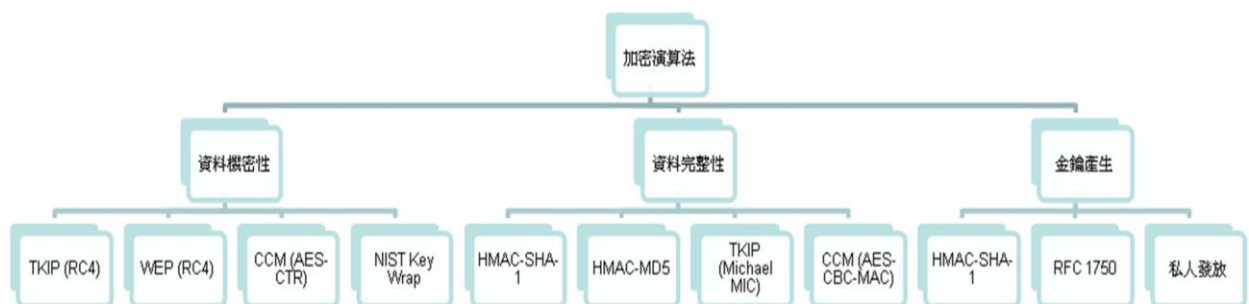
自從 IEEE 組織於 2004 年提出 IEEE 802.11i 修正版本後，IEEE 802.11 的安全防護技術主要可分為 Pre-RSN(Pre-Robust Security Networks) 與 RSN(Robust Security Networks) 2 大類。Pre-RSN 主要承繼原本 IEEE 802.11 標準的安全功能，其中包含開放系統鑑別、共享金鑰鑑別及有線等效加密(Wired Equivalent Privacy, WEP)機制，而 RSN 則修正 WEP 上的主要幾個安全缺失，並提供了更強固的資料完整性與傳輸機密性，例如 IEEE 802.1x 存取控制、可延伸鑑別協定(Extensible Authentication Protocol, EAP)、暫時性金鑰整合通訊協定(Temporal Key Integrity Protocol, TKIP)及計數器模式 CBC-MAC 通訊協定(Counter Mode / CBC MAC Protocol, CCMP)均是其相關安全核心技術，IEEE 802.11 安全防護架構詳見圖 16 所示。



資料來源：Recommended Security Controls for Federal Information Systems [2]

圖16 IEEE 802.11 安全防護技術架構

IEEE 802.11 安全使用之加密演算法詳見圖 17 所示。



資料來源：本計畫整理

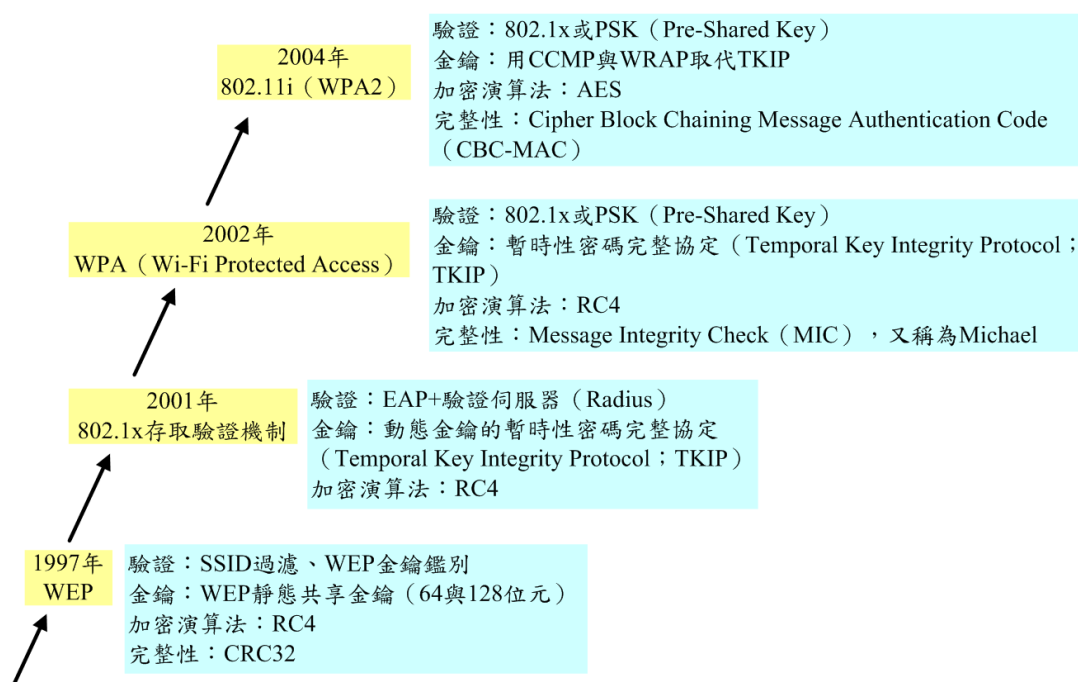
圖17 IEEE 802.11 安全使用之加密演算法

2.3.6.1 有線等效加密

有線等效加密(Wired Equivalent Privacy, WEP)又可稱為無線加密協定(Wireless Encryption Protocol)，主要用來保護無線區域網路資料安全的加

密機制。因為無線網路是以無線電波為媒介進行訊號的傳遞，此特性使得傳輸資料特別容易遭受竊聽。因此 IEEE 設計 WEP 加解密機制，希望讓無線網路使用者能夠獲得與傳統有線區域網路相當的資料傳輸機密性(這也是 WEP 的命名由來)。

不過以 WEP 為基礎的無線區域網路安全性機制並不完全，所以除了原本設計機構 IEEE 的持續改進與努力外，Wi-Fi 聯盟也陸續提出為業界接受的無線安全標準，從 2001 年後陸續出現 802.1x、WPA、WPA2 及 802.11i 等加強無線區域網路安全性的新標準，其中 IEEE 802.11i 為目前最新的無線區域網路標準，IEEE 802.11 安全性機制發展歷程詳見圖 18 所示。



資料來源： Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i，Bluetooth and Handheld Devices [3]

圖18 802.11 安全性機制發展歷程

●缺失：

雖然上市產品中，已有廠商把 128 位元與 256 位元金鑰加入其加解密機制

中，試圖以加大金鑰長度來增加攻擊的困難度，然而「金鑰長度太短」並不是破解 WEP 安全性的唯一因素，WEP 加密機制的主要安全缺失如後：

- 初始向量長度太短與廠商設計不良，導致只要能夠蒐集到足夠的封包數，並進行封包解析，即可以將金鑰輕易破解。
- 加解密用的金鑰長度太短，易被暴力攻擊法所破解。
- 缺乏適當的金鑰管理機制(如定期更新共享金鑰)，金鑰被竊取的可能性將大幅提升。
- RC4 金鑰產生演算法已經被證實不夠安全。
- 使用 CRC(Cyclic redundancy check)資料完整性檢核演算法，將使得封包完整性的安全防護不足。
- 單向的使用者認證問題(僅提供無線基地台對無線用戶端進行認證)，容易造成中間人攻擊。

2.3.6.2 Wi-Fi 存取保護(WPA/WPA2)

Wi-Fi 存取保護(Wi-Fi Protected Access , WPA)是由 Wi-Fi 聯盟業界團體所制訂的，主要是為加強第一代無線區域網路安全性標準 WEP 協定中，幾個嚴重的弱點而產生的過渡技術。

換言之，WPA 是在 IEEE 新版的無線區域網路安全標準 IEEE 802.11i 制訂完備之前，一個替代 WEP 的過渡方案，WPA 包括了 IEEE 802.11i 功能的大部分子集，Wi-Fi 聯盟透過發布 WPA 得以授令所有帶有 Wi-Fi 標誌的設備遵守 WPA 規範，並允許 Wi-Fi 網路硬體廠商在 IEEE 802.11i 正式發行之前，提供標準化的高安全選項。

WPA 在身分鑑別、機密性及完整性等安全性的加強如後：

●身分鑑別

WPA 將無線區域網路的驗證機制分為兩種模式，一般企業組織建議採用高安全性的 IEEE 802.1x 架構，小公司與個人 SOHO 族則建議採用較簡單且低安全的 Pre-Shared Key(以下簡稱 PSK)模式，讓每個用戶都使用同一個密碼。Wi-Fi 聯盟把這個使用 PSK 的版本叫做 WPA 個人版或 WPA2 個人版；用 IEEE 802.1x 鑑別的版本叫做 WPA 企業版或 WPA2 企業版。

●機密性

WPA 的資料是以一把 128 位元的金鑰與一個 48 位元的初始向量為基礎的 RC4 演算法來進行加密，WPA 比 WEP 安全，主要改進的地方就是使用可以動態改變金鑰的暫時性金鑰整合通訊協定(Temporal Key Integrity Protocol, TKIP)，並加上較長的初始向量，這將可以抵擋惡意攻擊者擷取與分析無線封包，進行 WEP 金鑰的破解之攻擊方式。

●完整性

WPA 對於所有傳輸資料的完整性也提供重大的加強與改進，原來 WEP 所使用的 CRC 技術在先天就不安全，因此 WPA 採用一種稱為 Michael 的訊息驗證碼，在 WPA 中正式稱為訊息完整性檢核(Message Integrity Check, MIC)。且 WPA 使用的 MIC 包含了框架計數器，可用來避免 WEP 的重送攻擊(Replay attack) 弱點。

為了降低風險，WPA 網路每當偵測到一個企圖的攻擊行為時，就會關閉 30 秒鐘。

綜合所言，WPA 利用 TKIP 將每一個封包都使用唯一的加密金鑰與更長的初始化向量，新增「經過簽署且不容易遭竄改或欺騙」的訊息完整性檢查值，並併入加密的框架計數器，以阻擾重送攻擊，再加上 WPA 所使用的加密演算法與 WEP 所使用的演算法也相似，所以可透過簡單的韌體升級

實作在既有的硬體上，不過 TKIP 亦存在一些潛在缺點，首先 TKIP 仍使用傳統的且日漸衰弱的 RC4 加密演算法，且動態金鑰更新過程需付出額外運算資源的代價。WPA 如何解決 WEP 上的安全弱點，相關內容比較詳見表 2 所示，詳細的加解密流程可參考無線網路安全參考指引。

表2 WPA 針對 WEP 安全弱點的因應方案

WEP 的弱點	WPA 處理弱點的因應措施
原 24 位元的初始向量太短	在 TKIP 中，將初始向量的大小擴充為 48 位元
資料完整性脆弱	WEP 加密 CRC-32 總合檢查碼計算已經由 Michael(設計用來提供增強式資料完整性的演算法)取代。Michael 演算法會計算出 64 位元訊息完整性編碼(MIC)值，然後再由 TKIP 加密這個值。
使用主要金鑰而非衍生金鑰	TKIP 和 Michael 使用由主要金鑰和其他的值所衍生出的一組暫時金鑰。此主要金鑰是由「可延伸的驗證通訊協定-傳輸層安全性」(EAP-TLS)或「受保護的 EAP」(PEAP)802.1x 驗證程序所衍生的。此外，透過封包混合函式輸入到 RC4 虛擬亂數產生器的秘密部分會隨著每個框架變更而改變。
無法重設金鑰	WPA 提供了自動重設金鑰以衍生出新的暫時金鑰。
無法抵抗重送攻擊	TKIP 使用框架計數器以抵抗重送攻擊。

資料來源：本計畫整理

●暫時性金鑰整合通訊協定(TKIP)

在 WPA 中所使用的加密演算法即為 TKIP，其主要的設計可相容於原本 IEEE 802.11 的硬體產品，可透過韌體與軟體升級來提高加密的安全。

一樣是透過 RC4 加密，但是可以讓每個封包都提供不同的加密金鑰值，且

原本的 WEP 加密使用 24 位元的初始向量值，目前的 TKIP 則使用 48 位元的初始向量值，如此可大幅減低初始向量值重複的機率問題。

雖然目前 WPA 的 TKIP 已經比起原本單純的 WEP 加密更為可靠，但這只是 WPA 第一個版本的方案，在 WPA 的進一步更新版本中，更採用了 AES 做為傳輸加密機制來增加安全防護強度。

WPA TKIP 相較於過去 WEP 加密，主要的不同在於過去是直接把收到的 WEP Key 作為加密的運算值，可是 WPA TKIP 並不是如此，而是將所收到的 Key 值，重新運算出加密的金鑰，在透過計算出來的加密金鑰進行後續加密的動作。WPA TKIP 相較於原本的 WEP 加密機制，不同之特點如后：

- 48 位元的初始向量值。

TKIP Per-Packet Key 加密機制，即每個 Packet 都產生不同加密的金鑰。

TKIP Per-Packet 金鑰產生流程可參考無線網路安全參考指引，在 TKIP 加密的機制下，會透過兩個階段產生之後要透過 RC4 加密的使用金鑰，而原本用來加密的 48 bits 初始向量值，被分為兩個部分(32 Bits 與 16 Bits)，分別在 Phase 1 與 Phase 2 的程序中參與加密金鑰的產生。

基本上 TKIP 的加密機制與 128-bits WEP 金鑰是一樣的，只是在於產生金鑰的方式不同，主要的差別就是 WEP 金鑰產生流程是把使用者輸入的 WEP 金鑰與初始向量值直接做為加密的 RC4 演算法金鑰值，可是對於 TKIP 而言，使用者所輸入的 TKIP Key 與封包的初始向量值都只是用來產生最後加密所用 128 bits 私密金鑰之參數，相對的也就提高安全性。

- MAC 位址過濾

很多無線區域網路設備中都會提供 MAC 位址過濾(MAC Address

Filtering)與認證功能，但 MAC 位址認證並不包含於 IEEE 802.11 安全標準中，只不過市場上的無線 AP 大多可以支援此功能。

其運作邏輯為無線 AP 可預先將合法使用者所用之無線區域網路卡實體位址，加入基地台的存取清單內，亦即事先設定好合法使用者的 MAC 位址名單，然後在用戶連線時進行 MAC 位址的比對來確認是否為有效的無線存取介面，此認證功能的主要目的是加強開放式與共享金鑰式的身分鑑別機制，進一步限制未經過授權的無線用戶端對網路進行存取的動作。但由於 MAC 位址容易被竊聽與偽裝，不肖之徒也可利用電腦自動變換網址嘗試來破解這層保護，所以單獨使用此技術並不安全。

– IEEE 802.1x 存取控制

IEEE 802.1x 於 2001 年 7 月獲得 IEEE 許可，這個標準定義以連接埠為基礎的網路存取控制架構，由 IETF 可延伸鑑別協定(EAP)發展而來的，可以用來實現乙太網路環境下的存取控制。

此種連接埠架構式網路存取控制是利用切換區域網路基礎結構的實體特性，來驗證連接到切換式連接埠的裝置，如果驗證處理程序失敗，就無法利用乙太網路切換式連接埠來傳送或接收訊框(Frame)，雖然這項標準原先是針對有線乙太網路所設計的，但是目前已被廣泛地應用於 IEEE 802.11 無線區域網路上，所以 IEEE 802.1x 被視為是目前無線區域網路上較安全的身分鑑別與金鑰管理協定。

簡單來說，IEEE 802.1x 是一種透過使用者憑證的驗證程序，來保護網路的一種連接埠存取通訊協定。一旦將 IEEE 802.1x 存取控制程序應用在無線區域網路環境中，即可大幅加強無線區域網路的安全性，如果有某個無線區域網路用戶端經由 IEEE 802.1x 驗證進行網路存取，一旦驗證通過，無線存取點就會開啟一個允許通訊的虛擬連接埠，反之，一旦授權不成功，就不會提供該虛擬連接埠，無線用戶端通訊就會受到阻擋而

無法連線。詳細的加解密流程可參考無線網路安全參考指引。

2.3.6.3 WPA2 新漏洞

近期無線網路加密通訊協定 WPA2 漏洞曝光，讓全球 Wi-Fi 加密連線都面臨高風險，這是比利時 KU Leuven 大學資安研究員 Mathy Vanhoef，在 2017 年 5 月時發現的一系列漏洞，他並設計了密鑰重安裝攻擊（Key Reinstallation Attacks, KRACKs）的概念驗證攻擊程式。

從無線網路標準加密標準來看，現今的 Wi-Fi 無線網路，為達到安全需求，普遍利用的是 WEP、WPA 及 WPA2 這三種。其中，WEP 是最早被公認為最不安全的，這是因為初始設計上有許多嚴重的弱點，即便沒有相關資訊專業知識的人，也容易取得工具程式，就可能在短時間內加以破解。

所以多數廠商建議是，不要使用 WEP 加密，最好使用相對較安全的 WPA2，因為這對於破解密碼的人來說難度更高。也因此，目前大多數裝置和 Wi-Fi 路由器，都依賴 WPA2 來加密 Wi-Fi 流量。

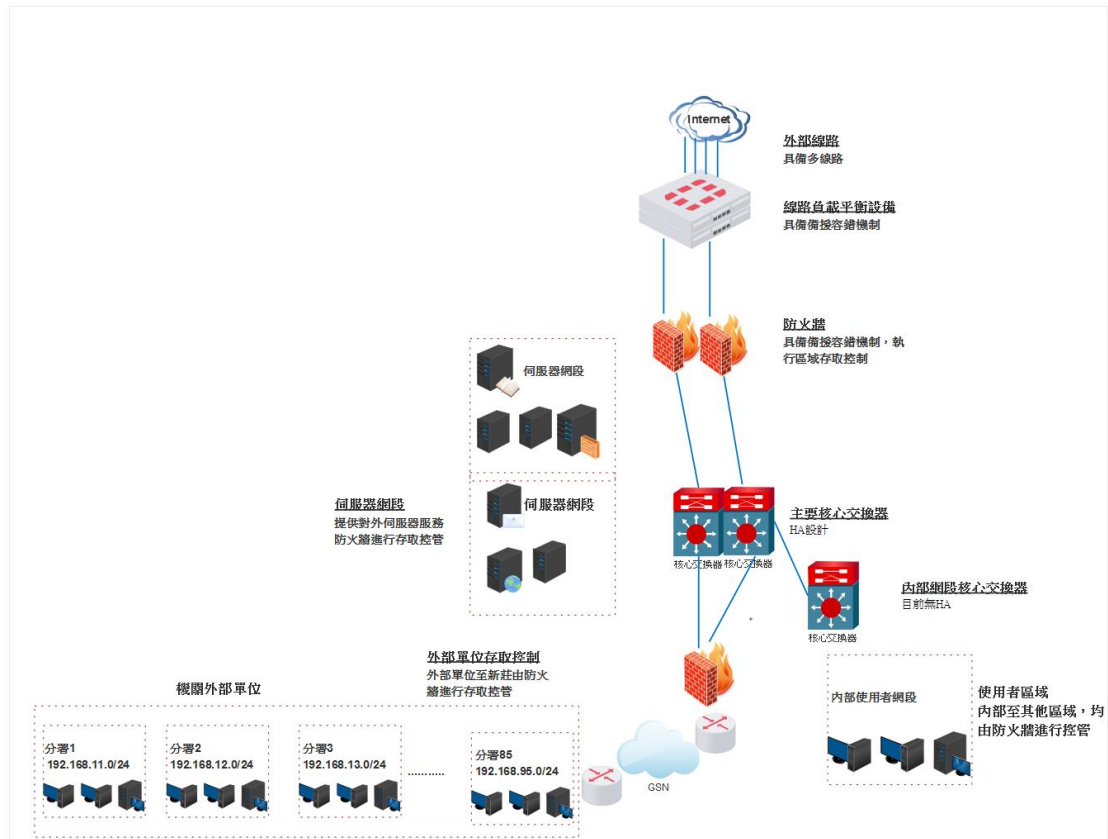
儘管過去也傳出不少 WPA2 被破解的消息，像是利用 WPS 漏洞或暴力密碼破解方式，但是 KRACKs 是不依靠竊取密碼的攻擊手段，直接針對 WPA2 協定本身的弱點，從終端裝置接入 Wi-Fi 進行連線交握的階段執行攻擊。

從原理來看，依據 WPA 2 無線網路加密的通訊協定，當終端裝置接入 Wi-Fi 時，在正式傳輸資料前，必須先經過四向交握（four-way handshake）這個階段，也就是要先經過四次溝通，以建立初始連線，以相互確認並產生所需金鑰，達成連線協議。而 KRACKs 攻擊就是利用此階段的邏輯缺陷，發現一系列漏洞。

2.4 部署原則

2.4.1 網路設備之組成

機關常見的網路架構與設備組成如圖 19 所示，分述如後：



資料來源：本計畫整理

圖 19 機關網路架構與設備組成

●對外線路設備

一般為 ISP 提供可能是小台的 ADUR、Router、xDSL 或光數據機。

●WAN 線路負載平衡設備

主要用於將兩條不同外線彙整，讓機關同仁同時使用，另當線路故障時也提供備援。

- 外部防火牆

主要區分區域間的存取，比如內部網路 IP 可連線非軍事區(Demilitarized Zone, DMZ)，但 DMZ 網路 IP 無法連線內部網路。

- 核心交換器

主要用於區分機關內各區域劃分 VLAN，以建立路由，提供區域間連線，機關內一般所有端點的預設路由 gateway 都會先到達核心交換器。

- 入侵防禦系統(IPS)

IPS 為網路安全設施，負責監視網路或網路裝置，能夠即時的中斷、調整或隔離一些不正常或是具有傷害性的網路資料傳輸行為。

- 內部防火牆

主要控管機關內部間存取，以設定 policy 方式，僅允許需要人員執行必要服務。

- 邊際交換器

負責收納端點電腦或設備，透過線路再連接至核心交換器。

2.4.2 網路區域劃分

機關網路區域的訂定是規劃部署網路架構的第一步，網路區域劃分主要的目的是清楚界定規劃不同屬性的區域，作為存取控制與安全規劃的基準群組。機關常見之網路區域劃分，如圖 20 所示，分述如後：



資料來源：本計畫整理

圖20 機關區域劃分圖

2.4.2.1 外部網路

機關對外網路區域，連接外部廣域網路(Wide Area Network, WAN)，此區域對內部需要經過防火牆的存取控制，非允許的服務與來源不能進入其他區域。

2.4.2.2 內部網路(LAN)

內部區域網路(Local Area Network, LAN)，主要是機關內部人員與內部伺服器。

2.4.2.3 非軍事區(DMZ)

DMZ 主要是放置機關對外服務伺服器，僅開放特定服務，同時需要嚴密控管此區域到內部區域的存取。

2.4.2.4 網路管理區域

網路管理區域，應明確標示網路的路徑及維運方式，網路設備維運應該與路由及服務的網段有所區隔，以避免當服務網段或路由網段被攻擊，進而影響網路設備的管理。

2.4.2.5 網路紀錄區域(Log)

備份主機(Backup Server)及紀錄(Log Server)存放的網段也應特別規劃，應避免除了設備備份與紀錄之發送以及管理員管理以外之連線行為。

2.4.2.6 實體隔離區域

機關依據特定需求可將部分區域執行實體隔離。

有關於上述網路安全區域之實體安全防護，宜納入於機關之整體資訊安全防護計畫之中，相關之安全控制措施請參閱「安全控制措施參考指引」之 5.11.實體和環境保護(Physical and Environmental Protection)內容。

2.4.3 機關 IP、虛擬區域網路(Virtual Local Area Network, VLAN)及路由的劃分

機關 VLAN 的劃分應該依據實際的需求，依據樓層、部門屬性、單位區隔、使用分界作為依據並進行適當的劃分，劃分的目的主要將不同屬性的群體做分隔，分隔後除了可以限定特定服務的傳遞外，也可以進一步進行不同 VLAN 間的存取控制，不同 VLAN 間的存取控制可以透過核心交換器存取控制清單(Access Control List, ACL)進行。

VLAN 劃分後再依據 IP 劃分進行彙整，則可以清楚確認機關中不同單位、樓層、部門分屬於那些 VLAN，以及其對應的 IP 網段與樓層。

- VLAN 與其對應的 IP 網段及單位樓層，詳如表 3 所示。其中針對不同單位大小切割不同 VLAN IP Subnet(256、128、64、32)。

表3 機關 VLAN 網段位置整理(範例)

	代號	位置	IP	VLAN
1	A	A1 單位	192.168.222.0/26	101
2	A	A2 單位	192.168.222.128/26	102
3	A	A3 單位	192.168.222.192/26	103
4	A	A4 單位	192.168.222.64/26	104
5	A	A5 單位	192.168.208.0/25	105
6	A	A6 單位	192.168.208.128/25	106
7	A	A7 單位	192.168.209.0/25	107
8	B	B1 單位	192.168.215.0/24	211
9	B	B2 單位	192.168.210.0/24	221
10	B	B3 單位	192.168.213.0/24	222
11	B	B4 單位	192.168.211.0/24	223
12	B	B5 單位	192.168.212.0/24	224
13	B	B6 單位	192.168.214.0/24	225
14	B	B7 單位	192.168.216.0/24	226
15	C	C1 單位	192.168.220.0/25	301
16	C	C2 單位	192.168.209.128/25	302
17	C	C3 單位	192.168.223.0/24	303

	代號	位置	IP	VLAN
18	C	C4 單位	192.168.221.32/27	304
19	C	C5 單位	192.168.221.192/27	305
20	D	D1 單位	192.168.45.0/26	402
21	D	D2 單位	192.168.45.128/26	401
22	E	E1 單位	192.168.221.0/27	501
23	E	E2 單位	192.168.221.64/27	503

資料來源：本計畫整理

路由劃分主要用以了解機關對外的路由規劃，透過管理表可以清楚確認對外的路由節點，機關對外的路由規畫可能為靜態或動態路由，平日應該清楚標註路由讓管理人員能夠確認，並定期更新，將整理結果留存，定期確認是否有差異，若有異動時再行增刪。

路由表管理以 A 機關為例，可分為 A 機關內部 VLAN 與其對應 IP 的整理、內部預設路由與指定路由確認、內部 OSPF 相關路由彙整確認、機關對外線路與其預設路由確認。

整理 A 機關負載平衡器線路資料詳如表 4 所示。

表4 A 機關負載平衡器

設備：線路負載平衡器
設備 IP 位置：10.1.1.253
路由設定：ISP 預設路由
中華電信網段： 211.72.195.1/0 211.72.195.254
GSN 網段： 60.248.154.1/24 60.248.154.254

資料來源：本計畫整理

A 機關對 B、C、D 機關防火牆路由資料詳如表 5 所示。

表5 A 機關對 B、C、D 機關防火牆

設備：對 B、C、D 防火牆
管理 IP：10.1.1.253
路由： 目前位址 192.168.64.0/18 Route 211.72.195.254
OSPF： 目前位址 0.0.0.0/0 Route 10.1.1.254

資料來源：本計畫整理

整理機關核心交換器 VLAN、對應 IP、路由，如表 6。

表6 A 機關核心交換器 VLAN 網段 IP 與路由

設備：A 機關核心交換器			
管理 IP：10.1.1.254			
目的位址		nexthop	路由
0.0.0.0/0		10.1.1.253	Static
192.168.64.0/18		10.1.1.252	Static
	位置	IP	VLAN
1	A 單位	192.168.11.254/24	11
2	B 單位	192.168.12.254/24	12
3	C 單位	192.168.13.254/24	13
4	D 單位	192.168.14.254/24	14
5	E 單位	192.168.15.254/24	15
6	F 單位	192.168.16.254/24	16
7	G 單位	192.168.17.254/24	17
8	H 單位	192.168.18.254/24	18
9	I 單位	192.168.19.254/24	19
10	J 單位	192.168.20.254/24	20
11	K 單位	192.168.21.254/24	21
12	L 單位	192.168.22.254/24	22
13	M 單位	192.168.23.254/24	23
14	N 單位	192.168.24.254/24	24
15	O 單位	192.168.25.254/24	25
16	P 單位	192.168.26.254/24	26
17	Q 單位	192.168.27.254/24	27

18	R 單位	192.168.28.254/24	28
19	管理網段	10.1.1.254/24	200

資料來源：本計畫整理

2.4.4 核心系統資料流程圖繪製

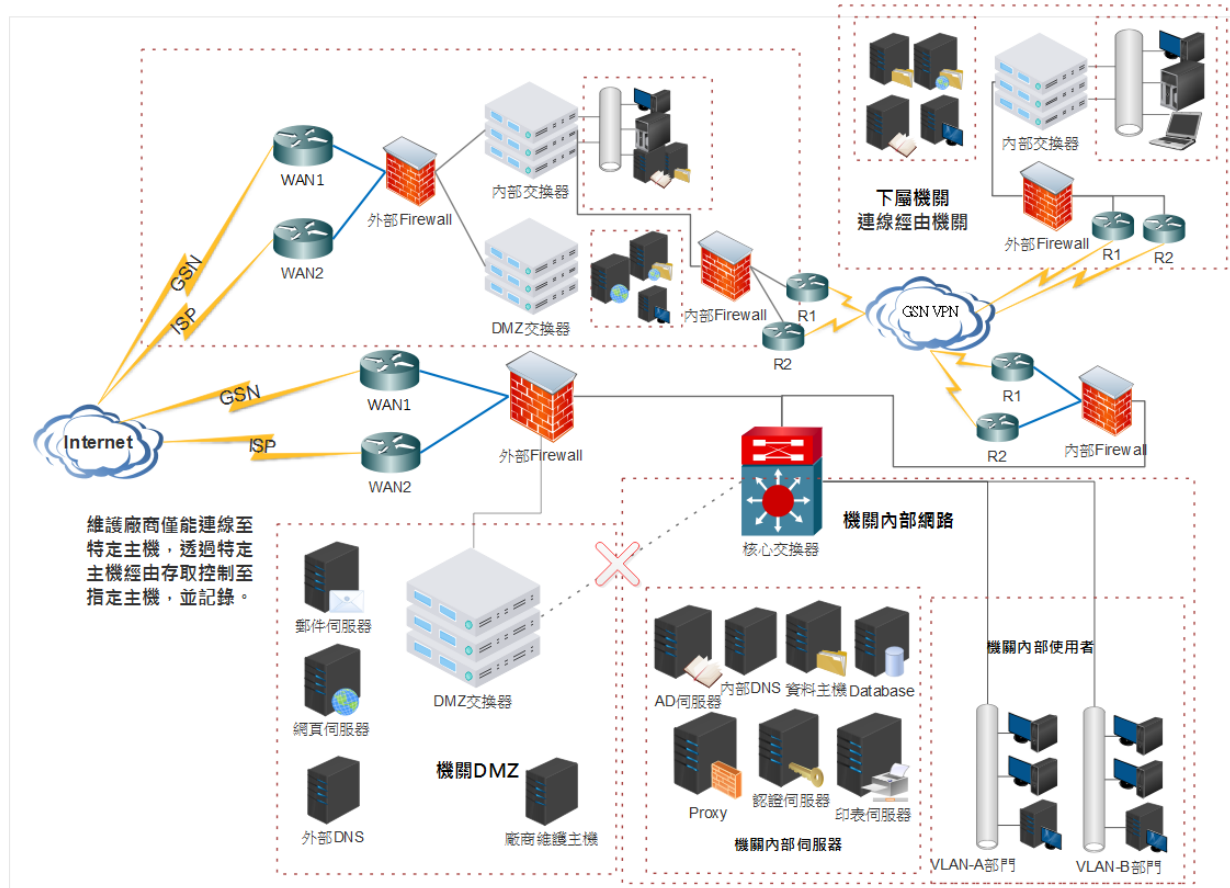
機關核心系統資料流程圖繪製，主要是先藉由核心資料流程的討論確認系統運作流程與流程細節。藉由使用情境確認核心系統的使用流程，使用流程圖可以協助機關檢視核心系統的資料流實際的走向，以確認完成的服務起始運作流程，配合實際邏輯與實體架構圖檢核，進而驗證核心系統是否符合原先預期的設計流程，同時藉由檢核結果了解實際運作現狀，據以判斷是否須調整優化流程或增加控制選項以加強安全性，另外藉由核心系統資料流程圖繪製，也可協助機關取得適當的流程方式，當機關需要建置其他重要系統時，可以依據此流程情境進行規畫安排。

2.4.5 機關區域間存取控制設定

機關區域間的存取控制檢測時，需要確認區域間的設備狀況，比如區域間是透過防火牆進行控管或是區域間直接經由核心交換器存取，詳見圖 21 所示。

一般 DMZ 至內部網路會規劃防火牆進行存取控制，部署時需要注意區域間的管理規則是否正確設定：

- 確認區域間管理規則有正確設定啟動，同時檢測條例是否有過多之現象、條例是否妥善控管、未使用的規則定期檢討刪除，並刪除不必要規則，以免累積後難以維護。
- 防火牆管制條例應備註說明此條例建立原因、用途、需求單位、設定/維護人員及建立/維護時間，以利管理並俾利交接。



資料來源：本計畫整理

圖21 機關區域存取控制圖

2.4.6 繪製機關網路架構圖

機關在部署完成 IP 網段規劃、VLAN 劃分、路由規劃、區域存取控制後，應依據上述資料繪製出機關網路架構圖，網路架構圖主要提供機關人員能夠簡單快速了解機關網路架構、線路狀態、備援狀態、重要節點網路設備、重要伺服器、區域分隔與對應 IP 網段、樓層 VLAN 分隔、重要設備實體位置標註，藉由網路架構圖達成上述的需求，協助管理者進行機關網路的維運。

機關的網路架構圖須具備邏輯網路架構圖與實體網路架構圖。

●邏輯網路架構圖

經由前述章節的彙整後，機關的 IP 網段規劃、區域劃分、VLAN 劃分、路由規劃、重要網路設備清冊均已經完成部署規劃，邏輯網路架構圖主要是將機關主要區域分隔，核心網路設備，邏輯連線方式，對外連線網路，上下行單位，進行繪製描述。讓機關人員或主管得以快速了解機關架構與區域分隔與不同區域間的運作流向，機關與上下行機關的相互關係。

●實體網路架構圖

實體網路架構圖的目的是將機關核心設備與主要架構中重要網路設備的實體連線方式與布置經由實體網路架構圖進行說明，實體網路架構圖中以線路的實體連接與重要設備的實際位置標註，核心網路設備的線路數目及其備援性，對外網路與對其他上下行機關線路的實體標註為重點，透過實體網路架構圖繪製可以協助管理者或主管確認上述事項，藉以釐清架構中的備援與容錯設計辨別設備的實體連線方式。

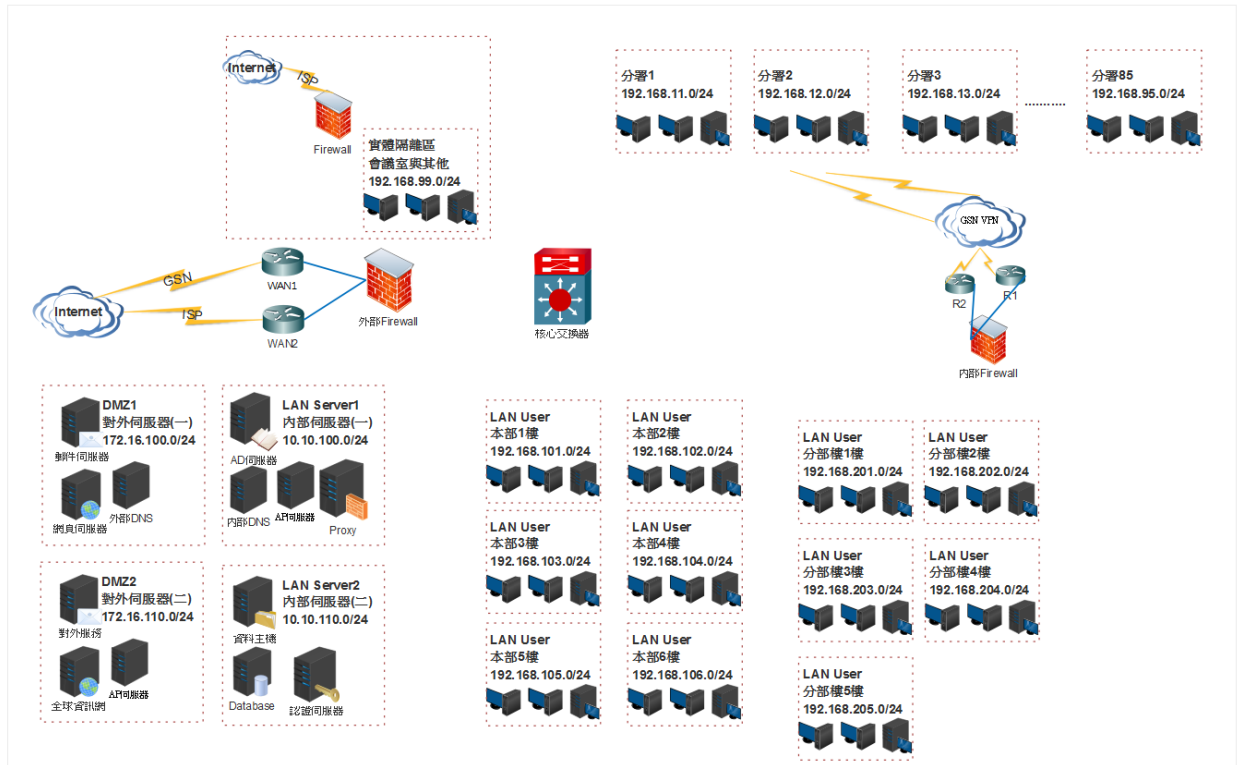
邏輯或實體網路架構圖在閱讀製作時應先繪製邏輯網路架構圖再由邏輯網路架構圖延伸說明。

網路架構圖可依據需求細分說明：

- 網路拓樸圖：包含重要節點防火牆、路由器、交換器設備。
- 網段拓樸圖：定義不同樓層或部門網段 VLAN 並以圖呈現。
- 伺服器架構圖：標示機關中伺服器的位置與區域，包含連接的交換器。
- 無線網路架構圖：標示無線網路架構與線路方式。
- 線路架構圖：標示機關對外線路顯示機關與上行下屬機關間的架構。

機關需要調查確認目前所轄網路型拓樸是屬於哪種型態，一般常見的型態大致分為環狀、星狀、樹狀、網狀、匯流排或混合式拓樸。

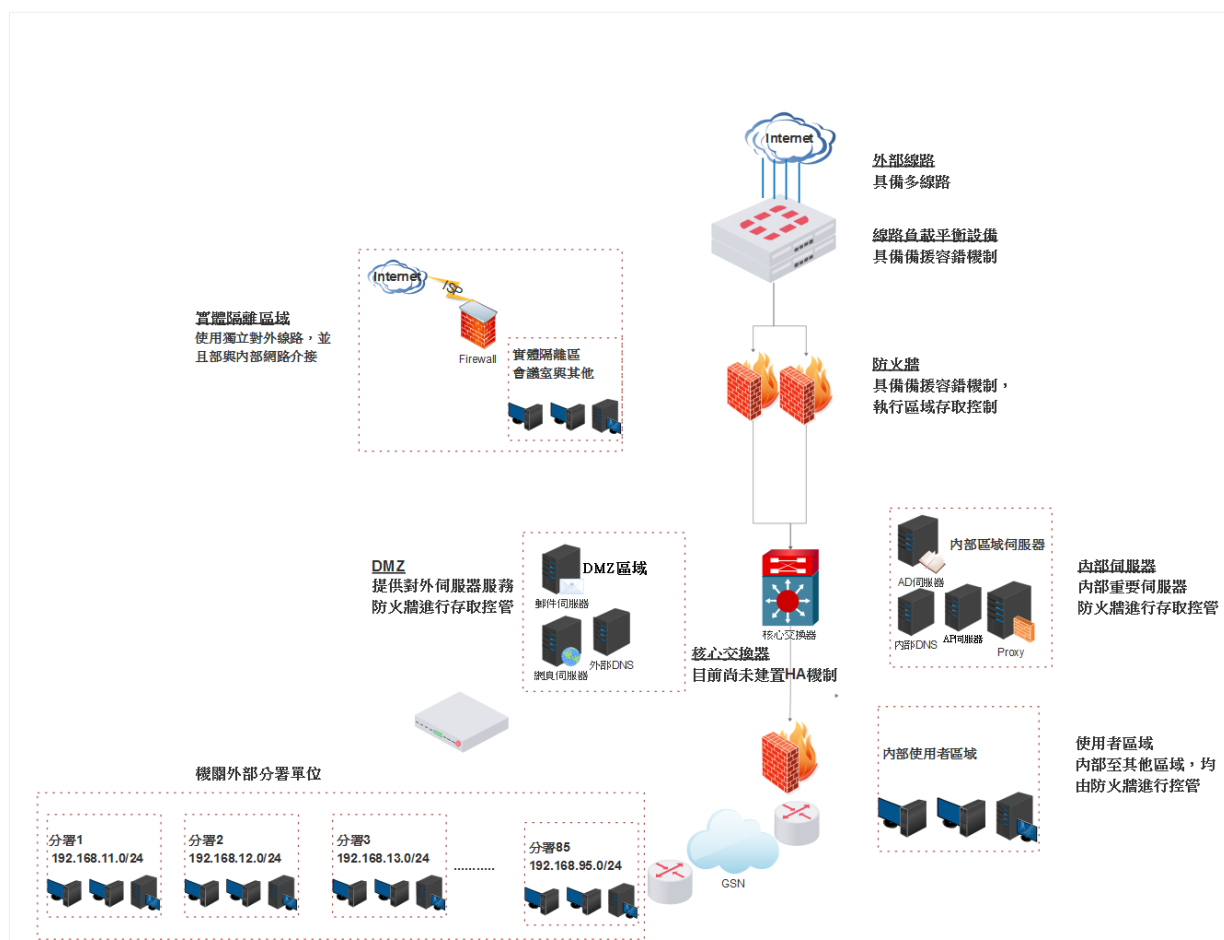
- 無論是何種型態主要需要確認目前實際的拓模狀況，透過拓模可以確認實際架構。
- 正確繪製邏輯網路架構圖：確認網路架構，並標明其型態，邏輯網路架構圖詳如圖 22 所示。



資料來源：本計畫整理

圖22 機關邏輯網路架構圖(範例)

- 實體網路架構圖建議呈現目前實際狀態：如節點、設備、電路、線路、伺服器等重要服務，詳如圖 23 所示。



資料來源：本計畫整理

圖23 機關實體網路架構圖(範例)

2.4.7 網路架構探查的呈現與監控

部署完成機關網路架構圖後，多數機關會透過管理軟體或設備探查既有重要網路設備，並呈現現狀，持續監控運作狀態，確認重要設備健康狀態與網路架構中重要節點的運行狀態。

機關管理軟體，可以依據前章節所述的不同拓撲圖依據管理軟體所能呈現的方式，儘量以相同的顯示方式，將機關彙整的不同網路架構圖於管理軟體中繪製並監控，藉以持續探查網路現況並監控重要設備，即時呈現反映問題。

2.4.8 比對檢核表，稽核檢測狀況

機關在部署完成後須檢測注意設備與架構狀態，例如：

- 對外線路設備，確認設備設定，定期備份，妥善保存 ISP 紙本資料。
- WAN 線路負載平衡設備，一般位於最外層，需注意線路使用優先權與分配，定期檢視線路頻寬使用趨勢。
- 外部防火牆，位於各區域網路間，需定期檢查管制條例，policy 建議分區顯示管理，比如將 DMZ 區域的 policy 集中，定期檢查條例數量，將閒置條例刪除，同時針對所有條例應該備註其用途與建立人員。
- 核心交換器定期備份，檢查設定是否有異動，檢測 interface 健康狀態，如果有光纖介面也需要確認 GBIC 的使用狀況評估是否需汰換。
- 入侵防禦系統通常位於最外端，一般用以屏蔽外部攻擊，若機關有設備，需定期確認是否持續有事件，正常狀態下，每天應該都有多筆不同等級事件偵測。
- 網頁應用程式防火牆(Web Application Firewall, WAF)，一般擺設於重要伺服器前做為屏蔽，多以對外網站為主，需定期注意運作狀況，定期檢測報表，針對可能威脅進行處理。
- 內部防火牆，擺設於內部機關間，定期檢查條例數量，將閒置條例刪除，同時針對所有條例應該備註其用途與建立人員。
- 邊際交換器，定期備份，檢查設定是否有異動，檢測 interface 健康狀態，如果有光纖介面也需要確認高速乙太網路介面轉換器(Gigabit Interface Converter, GBIC)的使用狀況評估是否需汰換。

部署完成後可依機關需求訂定網路檢核表檢測部署狀況，亦可參閱 3.1.7 網路架構規劃查檢表與細項說明訂定機關之網路檢核表，審視網路部署情形。

檢核表用以檢核規劃部署架構或是針對已經運行的機關架構進行檢核評估。

2.4.9 常見錯誤樣態與架構歸納

依資安會報執行資安稽核結果，歸納網路常見錯誤樣態分述如後，機關於執行網路規劃，宜避免該等錯誤，或檢視現行網路架構時，宜確認是否有符合常見錯誤樣態情事，若有則併入建議處理事項。

機關網路架構常見錯誤樣態，詳見表 7 所示。

表7 機關網路架構常見錯誤樣態

項次	錯誤樣態	可能影響	備註
1	使用者、遠端 VPN(虛擬私人網路通道)網段與內部伺服器網段未進行區分。	使用者可能存取未授權的資源	參考 2.4.2 2.4.5
2	放置 Web 伺服器的 DMZ 網段可直接存取 AP 伺服器(應用軟體伺服器)與資料庫伺服器(資料庫伺服器)所在的內部網段，未經過適當的存取控制。	DMZ 可存取內部，當 DMZ 遭受入侵時可能藉此進入內部網路。	參考 2.4.5
3	未適當區分區域，例如 DMZ 區為對外網路，內部網路宜區分為開發區、測試區、上線區。	上線區與測試區或開發區未予區隔，當測試區或開發區若有異常時，可能影響上線作業。	參考 2.4.2 2.4.5
4	對網際網路僅具備單一線路，未規畫故障備援機制。	當聯外線路故障時，會造成對內外間服務連線中斷。	參考 2.4.1 2.4.2
5	未區分 VLAN，將所有使用者與伺服器置於同一 VLAN 中。	無法針對伺服器進行適當存取控制。	參考 2.4.2 2.4.3

資料來源：本計畫整理

機關存取控制常見錯誤樣態，詳見表 8 所示。

表8 機關存取控制常見錯誤樣態

項次	錯誤樣態	可能影響	備註
1	內部網段之間未配置存取控制。	使用者可能存取不需要的資源。	參考 2.4.5 3.1.5
2	WEB(網頁伺服器)、AP 伺服器與 DB 伺服器之間未使用 ACL 進行控管。	造成安全疑慮與可能產生之非必要存取。	參考 2.4.5 3.1.5
3	開發區、測試區、上線區之間未設置存取控制。	可能造成各區域間存取不需要的資料，測試區相對易發生異常，未適當區隔容易對上線區造成影響。	參考 2.4.2 2.4.5
4	非內部電腦放置於內部電腦專屬網段	非內部授權電腦可能存取內部資源，造成資料外洩等問題。	參考 2.4.5
5	網路設備使用本機認證。	無法透過其他機制作強制定期更換密碼等控管。	參考 2.4.3 2.4.5

資料來源：本計畫整理

網路備援常見錯誤樣態，詳見表 9 所示。

表9 網路備援常見錯誤樣態

項次	錯誤樣態	可能影響	備註
1	網路設備僅有單台設備提	會有單點失效服務中斷	參考 2.4.1

項次	錯誤樣態	可能影響	備註
	供服務且對外線路並無備援電路。	之情況。	2.4.2
2	部分網路設備僅透過一台機房主機 Console 連入。	當操作機房主機故障時，無法進行相關服務與維護。	參考 2.4.1 2.4.2
3	底層 switch 至核心交換器僅有一條線路提供服務。	當線路故障時會造成該區域服務中斷。	參考 2.4.1 2.4.2

資料來源：本計畫整理

機關防火牆常見錯誤樣態，詳見表 10 所示。

表10 機關防火牆常見錯誤樣態

項次	錯誤樣態	可能影響	備註
1	DMZ 防火牆規則對內網全部開通。	DMZ 區域可能淪為攻擊內部網路的跳板。	參考 2.4.5 2.4.8
2	防火牆 policy 紊亂、policy 筆數過多，未適當註解用途。	無法清楚確認 policy 用途並作適當增刪。	參考 2.4.5 2.4.8
3	防火牆 DMZ 區域對外連線除黑名單外，允許所有往外的連線。	DMZ 伺服器可能對外傳輸不必要資料。	參考 2.4.5 2.4.8
4	外層防火牆設備、網路交換器、負載平衡器 WebUI 與 SSH 未限制可存取的網路位址。	外部人士可進行惡意登入測試，內部非授權人員亦可能出現不當登入之行為。	參考 2.4.5 2.4.8

資料來源：本計畫整理

網路傳輸常見錯誤樣態，詳見表 11 所示。

表11 網路傳輸常見錯誤樣態

項次	錯誤樣態	可能影響	備註
1	與合作廠商間、外部的使用者、其他機關等之網路傳輸，未使用加密之傳輸協定，例如：簡單檔案傳輸協定 (Trivial File Transfer Protocol, TFTP)、SSH、https 等	容易遭受資料側錄，以進行資料竊取。	參考 2.4.5 2.4.8

資料來源：本計畫整理

3. 管理程序

3.1 「規劃」

3.1.1 導入前置需求

機關在進行建置前需要針對機關的部門、單位、樓層、服務屬性、群眾服務需求等進行了解，依據實務需求與機關資訊人員進行討論，方便機關管理人員進行規劃。管理人員規劃時，須確認不同單位的端點需求，規劃足夠的 IP 並且預留足夠空間提供未來擴編使用，進行調查時，則要針對不同部門的人數以及服務需求，並了解其日常存取的特性以及對應的伺服器需求，並確認是否有其他特殊需求，如外部遠端 VPN、特殊伺服器存取需求。

透過訪查資訊彙整需求，條列單位窗口、設備清單，包含閘道設備、路由器、交換器、伺服器、端點設備，作為 IP 設定資料與區域劃分、VLAN 劃分及路由規劃的基本資料，進行後續實際規劃時的參考依據。

有關於網路架構之安全等級宜參考「資通安全責任等級分級辦法」之資通系統防護需求分級原則，評定機關核心資訊系統，取其最高者，用以律定網路之安全等級。

3.1.2 IP 設定與區域劃分

依據訪查所得的單位需求，進行 IP 設定資料與區域劃分，劃分方式可參閱 2.4.1 列表先進行單位與樓層的規劃，逐一確認。完成後再與需求單位比對實際端點人數是否相符，預留的空間是否足夠未來擴編調整使用，區域的劃分是否符合後續存取控制的需求。

IP 的規劃與設定，需標註 IP、子網路遮罩、閘道位置、樓層、部門、VLAN、對應的區域，以方便做後續管理應用。

3.1.3 VLAN 與路由規劃

在 IP 與網段區域劃分完成後，管理者應該依據劃分的結果設定適合的 VLAN，並將結果彙整整理為表格，方式可參閱 2.4.3 彙整。

完成彙整後，則可清楚理解機關 IP、網段、區域分隔、VLAN 劃分間的關係，再確認機關路由規劃。此處所述的路由規劃，包含機關不同 VLAN 間的路由規劃，機關若採靜態路由，則應清楚標註；若使用動態路由則須說明路由方式。機關對外的路由規劃也應該詳細標註，包含路由方式與備援方式，方式可參閱 2.4.3 彙整。



3.1.4 機關資料流程圖繪製

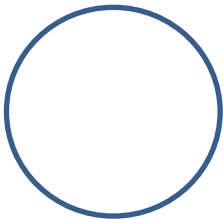

資料流程圖(Data Flow Diagram , DFD)是描述系統中資料流的一種圖形工具，它標示出一個系統的邏輯輸入和邏輯輸出，以及把邏輯輸入轉換邏輯輸出所需的加工處理。應注意的是，DFD 不是傳統的流程圖，資料流也不是控制流。DFD 是從資料的角度來描述一個系統，是系統發展生命週期中之「結構化系統分析與設計」所使用的標準描述工具之一。

3.1.4.1 資料流程圖基本圖形符號

資料流程圖有以下四種基本圖形符號，是常用的流程圖繪製工具中，所用符號最少的一種，詳見表 12 所示。

表12 資料流程圖之符號說明

符號	說明
	表示資料的來源或利用之去向，代表所描述系統以外之其他系統或是以外之其他系統或是外部個體。
	表示資料的流動路徑，若有需要可將資料名稱標示在箭頭符號的上方

符號	說明
	表示一個個體或是流程，資料流入經此程序處理之後，轉換成流出資料。
	代表儲存資料的地方，通常是檔案或是資料庫。

資料來源：本計畫整理

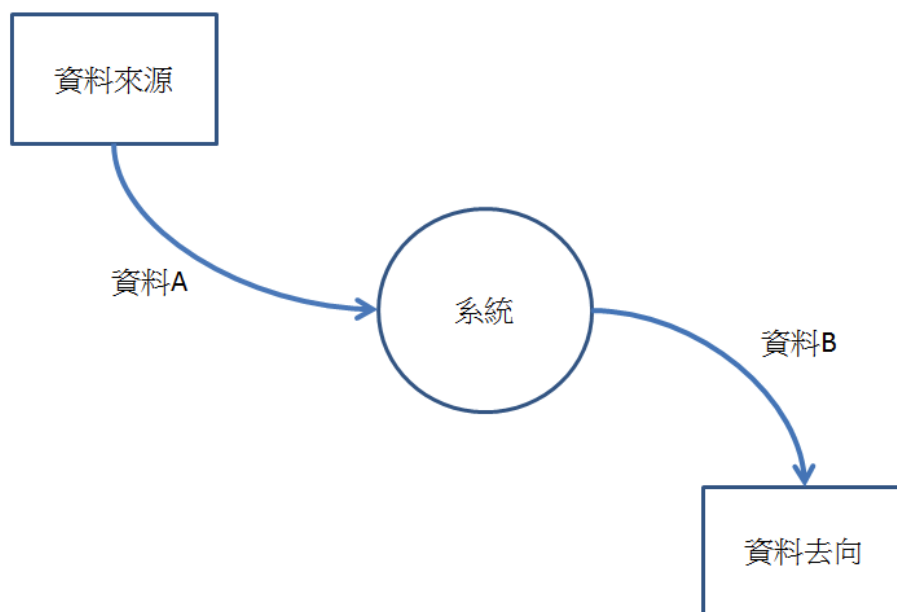
3.1.4.2 資料流程圖的繪製要領

為了降低系統的複雜性，一般採取「逐層分解」的方法，繪製分層的 DFD。

一般原則是：先全局後局部，先整體後細節，先抽象後具體。

繪製分層 DFD 的步驟一般是：

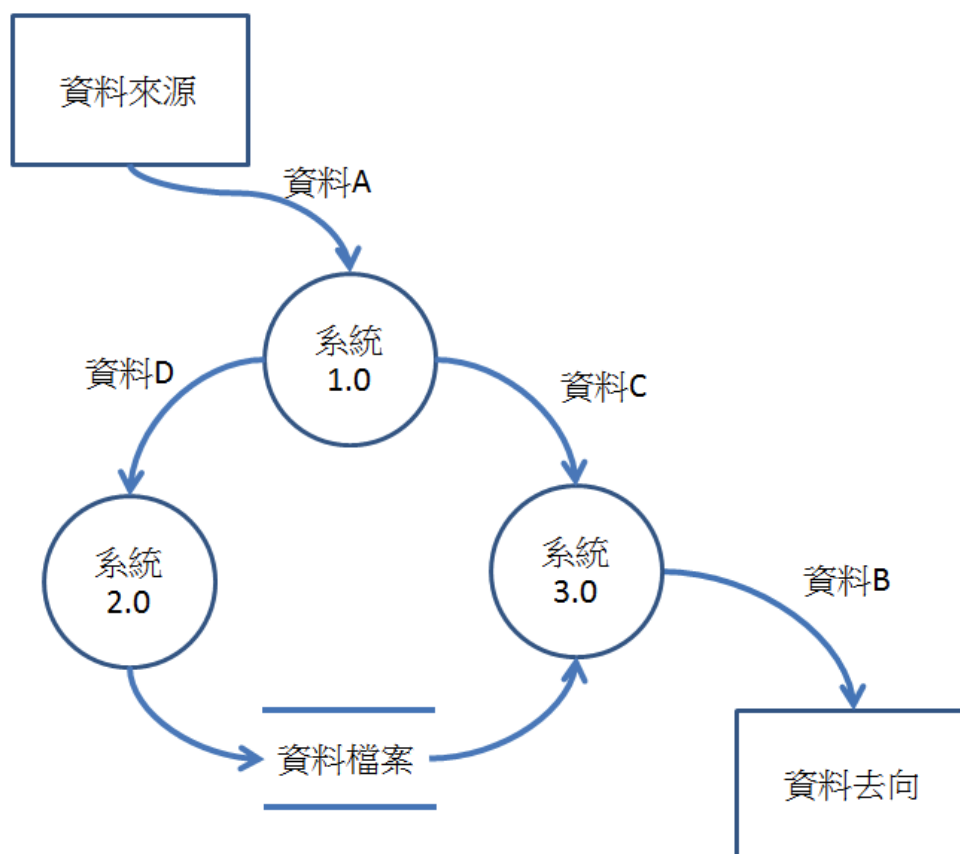
先確定整個系統的範圍和功能，繪製最頂層的 DFD，又稱之為背景圖，主要由一個資料來源，經過一個系統處理之後，再標示資料之去向，範例詳見圖 24 所示。



資料來源：本計畫整理

圖24 DFD 背景圖範例

繪製出頂層的 DFD 之後，然後逐層分解頂層 DFD，可獲得若干中間層 DFD，第 0 階資料流程圖範例，詳見圖 25 所示。



資料來源：本計畫整理

圖25 第 0 階資料流程圖範例

- 根據獲得的中間層 DFD 繪製，繼續繪製各個底層的 DFD。

本指引應用 DFD 於機關核心系統資料流程圖繪製，主要是先藉由核心資料流程的討論確認系統運作流程與流程細節，同時藉由檢核結果了解實際運作現狀，判斷是否須調整優化流程或增加控制選項以加強安全性。

規劃階段機關可提供資料流程圖繪製的情境範例，引導各核心資訊系統管理人比照情境範例，製作各核心系統資料流程圖，描述資料流如何運行，說明資訊傳遞與儲存，藉此流程了解核心系統實際運作情形。

稽核人員可以依據機關所提供的資料流程圖進行檢核確認，檢核方式可以依據檢核表進行驗證。

3.1.4.3 DFD 類型

DFD 按其資料及流程所描述之方式，又可區分為以下二種類型

- 實體資料流程圖(Physical DFD)

圓形圖示表示處理資料的人、地、物等實體，以名詞表示。

- 邏輯資料流程圖(Logical DFD)

圓形圖示表示處理資料的程序，以動詞表示。

本指引建議採用實體資料流程圖之要領繪製，藉以瞭解機關核心資訊系統與網路架構之關連。

3.1.4.4 DFD 檢核要領

DFD 的繪製必須遵守「流入與流出上下層一致」的原則(A set of Balance DFDs)，以圖 24 為例，背景圖中所描述之系統範例有資料 A 流入，資料 B 流出，則次一層的第 0 階資料流程圖(圖 25)，也必須遵守資料 A 流入，資料 B 流出之原則。

本指引建議應用 DFD 作為瞭解機關網路架構之關連，並非作為系統開發與設計之用，而是繪製出第 0 階資料流程圖作為網路架構分析之參考。

3.1.5 網路區域間存取控制

3.1.5.1 網路區域的訂定

進行存取控制規劃前，應先訂定機關之網路區域，訂定的方式如 2.4.1 所述。

3.1.5.2 管理規則規劃

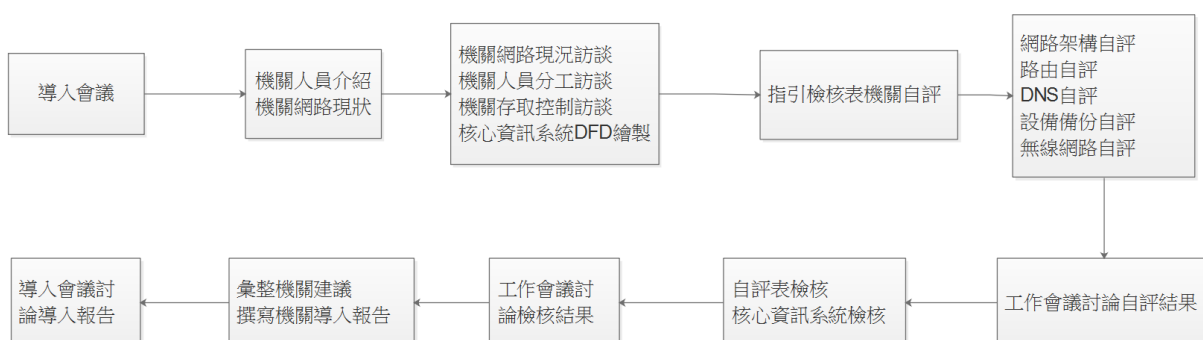
網路區域間的存取控制在完成規劃後，管理者應該條列不同區域間的存取

規則，比如 DMZ 到內部網路，那些主機的那些服務可以使用，或是那些人員或端點能夠存取特定主機的重要服務。存取控制是機關內資訊安全的重點項目，在規劃時應該將所有管制存取控制規則詳列，例如：管理規則的來源位址、目的位址、網路服務類型，清楚標示存取控制的內容與方向性(指網路資料之流向)，在建置前逐一討論，建議使用正面表列，即未在允許規則列表內的服務一律封鎖。

區域間存取控制列表應該以表格方式詳列管理需求，並依據表格檢驗設備中的管理規則是否依據規劃表格執行，才能正確管理，正確性包含表內的存取控制內容、順序、說明。

3.1.6 檢測流程規劃

在規劃後執行前，須檢測規劃流程是否符合所有討論建議內容，由區域劃分與 IP 規劃先進行確認，進而檢查路由規劃是否正確，有無提供備援機制，確認後再針對存取控制進行檢測。檢測原則先檢查架構，再確認區域，接著檢查存取控制是否落實，同時也測試有關加密(如無線)是否安全設定。檢核確定流程中各項目若有遺漏處應該予以補足，至各項目皆完整後再進行執行，機關網路架構檢核導入流程規劃可參考圖 26 所示。



資料來源：本計畫整理

圖26 機關網路架構檢核導入流程圖

3.1.7 檢測項目細項說明

檢測項目主要是針對機關網路架構中重要的項目進行彙整，提供機關在部署、規劃時能參考「網路架構規劃」安全控制措施查檢表(以下簡稱查檢表)詳見附件 1 所示，針對網路架構中不同項目進行確認，包含網路架構檢核表、路由檢核表、DNS 安全性檢測、防火牆檢核表、網路設備備份檢核表、無線網路檢核表。

3.1.7.1 網路架構檢核項目

3.1.7.1.1 網路架構資料檢核

- 邏輯網路架構圖

檢查是否有邏輯網路架構圖，標示網路區域的邏輯關係，方便了解網路架構。

- 實體網路架構圖

檢查是否具備實體網路架構圖，了解實際網路架構與設備的地點、區域、樓層、部門、單位。

- 網路架構圖具體呈現網路現狀

網路架構圖是否具體呈現網路現狀，透過邏輯與實體架構比對確認資料是否能協助管理者釐清架構。

- 架構圖包含重要設備如防火牆、核心交換器、重要伺服器

檢查架構圖中是否包含重要的網路設備與伺服器，並能顯示出其相對位置區域。

- 具備管理軟體

檢查是否具備網路管理軟體，並確認是否完整設備納管重要設備。

- 管理軟體可適當呈現網路狀態，反映目前現狀

確認管理軟體能否呈現網路狀態，反映實際現狀，並妥善納管重要設備，同時可以即時呈現網路異常，協助管理者掌控核心設備狀態。

- 管理軟體可分區域呈現

管理軟體是否可以分區呈現不同區域的網路現狀。

3.1.7.1.2 IP 與區域的配置

- 各主機 IP 配置圖、網路設備放置位置

是否具備資料顯示 IP 配置與網路設備的位置，是否具備清冊資料供管理使用。

- 各區段(含 IP)網路架構圖、各網段連線方式

網路架構圖中，資料是否也顯示對應區域的 IP，與不同網段間的連線方式。

- 網路 IP 配置清冊、網段與樓層或單位清冊

是否具備 IP 配置完整清冊，包含 IP、樓層、單位，可供管理查詢。

3.1.7.1.3 線路備援

- 對外線路具備備援線路

確認機關對外線路是否具備備援機制，當主線路失效時能可銜接運作，若無，是否有其它預防補救措施。

- 核心交換器至邊際交換器具備備援線路

核心交換器或是邊際交換器是否具備備援線路，避免單一線路故障時仍能運作，若並非全部均有備援網路，宜有備註說明。

- 重要網路設備具備線路備援

重要網路設備是否具備備援線路，避免單線失效時仍能接替運作，若針對重要網路設備有備援線路請加註說明。

3.1.7.1.4 容錯備援

- 重要網路設備是否具備容錯功能

針對重要網路設備是否具備容錯機制，當設備故障時能直接接替處理。若不具備容錯功能，則可說明是否存在備品設備，當設備故障時，能快速將設定匯入備品設備中接替運作。

- 重要伺服器是否具備容錯功能

針對重要伺服器是否具備容錯機制，當設備故障時能直接接替處理。若不具備容錯功能，則可說明是否存在備品設備，當設備故障時，能快速將設定匯入備品設備中接替運作。

3.1.7.2 路由檢核表

3.1.7.2.1 路由資料備份與說明

- 路由資料備份

針對重要路由資料具備資料備份。

- 路由資料說明

針對路由的使用說明有文字註解，藉以了解路由用途。

3.1.7.2.2 路由資料合理性檢查

- 路由資料使用維護更新

確認路由資料有定期更新維護，並汰除未使用與不合理的路由項目。

- 動態路由狀態與事件確認

在動態路由的環境下，確認有定期檢視動態路由運作是否有異常事件發生，確認運作中斷或異常事件。

- 不存在非機關核可路由

確認設備不存在非機關核可路由。

3.1.7.3 DNS 安全性檢測

3.1.7.3.1 DNS 主機檢測確認

- 無非核可主機安裝的某個套件軟體有開啟 DNS 服務

確認管理的主機可能被利用當成跳板的原因，不限於 DNS 伺服器，確認是否有一般伺服器被開啟 DNS 功能，或主機安裝的某個套件軟體有開啟 DNS 服務。

- 核可主機設定良好的存取權限

主機為機關授權的 DNS 伺服器，確認是否設定良好的存取權限。

- 依據規定執行經常性的弱點漏洞管理與修補

主機可能已被入侵，並安裝惡意軟體與開啟 DNS 服務。

- 內部 DNS 安全調整檢測

機關內部 DNS 安全調整檢測，建議加強下列事項：經常性的弱點漏洞管理與修補、落實存取管控機制、補強管理資訊與記錄、提升 DNS 自身防護能力。

- 外部 DNS 安全調整檢測

機關外部 DNS 安全調整檢測，同前項，惟面對眾多類型 DNS 惡意攻擊，機關一般的防火牆或相關設備很難完整防禦，建議可將對外 DNS 託管於 TWNIC 或政府網際服務網(GSN)。

- 外部 DNS 設定託管，並妥善設定

建議機關可將其對外 DNS 服務轉移至 TWNIC 或 GSN 專人管理，網管人員可透過網頁管理各自的網域，託管單位一般也能提供較好的防護。

- 關閉不必要的 DNS 服務

建議機關網管檢查並關閉伺服器上不必要的 DNS 服務，同時防火牆 policy 也需要針對 DNS 進行控管，關閉不需要的 DNS 服務存取。

3.1.7.4 防火牆檢核表

3.1.7.4.1 防火牆管理方式檢核

- 管理介面採用圖形化介面(graphical user interface, GUI)或 web 方式，並以加密連線

管理連線方式確認，確認設備管理方式同時檢測管理連線是否有啟動加密，以確保連線安全。

- 僅允許特定 IP 執行管理方式設定

管理方式限制來源 IP，透過實際確認可防止非法管理人員由未核准的端點連線，降低管理風險。

- 管理設定不允許採遠端存取方式執行

檢測是否開啟外部連線，一般管理情境上不應開啟對外管理連線，若有必要，則可透過 VPN 或其它加密驗證連線進行，而非直接開啟對外連線。

- 管理帳號依據機關人員權限身分建立

管理帳號應當依據管理權限建立，依據機關管理稽核設定讓不同管理者使用不同帳號。

若設備具有多層管理認證登入功能，可評估進行第三方身分認證管理方式(如雙因子認證)以確保為管理者本人登入操作與管理。

- 應具備唯一識別及鑑別機關使用者，不應有共用帳號之行為

檢查是否有多人使用同一帳號，機關網路設備不應多人使用同一帳號，避免設定混淆，權限不分。

- 管理帳號未結合 AD 或身份伺服器

管理帳號不建議結合 AD 或其他身分伺服器，避免遭破解時，衍生全面性的風險。

- 管理帳號密碼複雜度應符合機關要求

帳號管理/刪除臨時/緊急帳號：機關所規定之資訊系統各類型帳號有效期間已逾期，資訊系統應自動地選擇刪除或禁用臨時和緊急帳號。

備註：這項強化控制措施，應於已經超過預先定義的時間，自動刪除臨時和緊急帳號，而非系統管理員方便的時候。

帳號管理/禁用閒置帳號：超過機關所規定之有效期間時，資訊系統應自動禁用閒置帳號。

帳號管理/閒置登出：當超過機關所規定之預期間置時間或機關登出的時候，機關應要求使用者登出。

- 設備校時設定正確運作

應於伺服器機房設置校時系統。

管制 NTP 連線。

- 管理 SNMP 存取，限制存取 IP 並改除 public

3.1.7.4.2 防火牆管理規則檢核

- 針對 open all[Allow any/all]的管理規則有控管與說明，確認使用需求之必要性

針對 open all 的管理規則有控管與說明，透過 policy 檢測確定規則必要性，同時定期檢視使用狀況。

同時檢測是否存在超過實際需求範圍的管理規則，比如檢查來源與目的的 IP 範圍是否過大、開通的服務 Port 是否有過多或全開的狀況。

- 管制規則定期查核更新汰除

管理規則過多容易造成條例管理不易，檢測規則是否可以簡化。管理上應該定期檢查規則，確認並汰除未使用的規則。

管理規則檢核可以依據機關需求制訂檢核週期，建議至少每季檢核一次。管理規則檢核人員宜與網路管理人員區分，以落實檢核。

- 管制規則合理設定，不存在邏輯式的衝突

檢查管理規則的合理性，並確認不存在不合理的管理規則，若有宜調整刪除。

管理規則異動應建立申請審查機制，具備申請及准駁之規定。由審查人員確認所申請規則的合理性，經由主管核可後由防火牆管理員開通，短期性開放或變更須敘明原因與啟始期限，並留存文件備查。

同時納入規則使用率判斷，依照規則的使用率，調整防火牆規則先後順序，以提升防火牆處理效能。

管理規則異動應建立申請機制，須可申請及准駁之規定，短期性開放或變更須敘明原因與啟始期限，並留存文件備查。

- 管理規則清楚註解說明

管理規則應該加註使用說明或建立者，方便機關不同管理者間進行確認，同時也能清楚確認規則的建立者與使用用途。

- 管制規則依據實際需求細分，按照區域條列整理

管理規則應依據實際需求或區域細分，以便於管理，檢查是否符合。

同一區域管理規則：網管 IP → 網管設備 IP → 其他防火牆管理 IP → 阻斷全部連線。

- 區域間妥善分隔管理

不同區域間應該透過規則加以限制，應檢查不同區域間是否適當阻隔。

區域規則：存取量大的網路區域往上設定；存取區域連線數不大者，往下設定。

- 來源或目的群組等物件正確設定

檢查來源目的的物件或群組是否有正確設定，包含子網路遮罩是否設定過大，造成來源或目的位址的錯誤。

- 管制規則物件需製定固定格式，以利管理與設定

管理規則中的任一物件變數，需訂定固定格式（ex: 172.16.1.0-24_HQ-2F-OAsub; 172.16.1.1_HQ-2F-Printer）。

- 最後一條管制規則應阻斷不合規的所有連線(Deny any/all)

阻斷其他 IP 連線防火牆，加強防火牆本身安全。

3.1.7.4.3 防火牆設定備份與 log 紀錄

- 分析過濾異常連線紀錄(Alert Log)，並將一個月內網路設備紀錄檔集中至 Log Server

是否針對設備異常連線紀錄進行備份紀錄並集中至伺服器，方便後訊續問題的查詢。

- 收集近一個月管理人存取紀錄及帳號權限(Access log record)

針對防火牆管理人的帳號進出與存取是否有紀錄存取。

- 備份設備管理規則 (Policy)

機關應訂立流程於固定時間或設定異動時進行備份，並針對管理規則匯出備份同時加註文字說明。

備份時，應做完整性檢查，並確認備份資料是否正確，如檔案大小與前次是否接近，隨管理規則增多時檔案應微幅增大。

完整備份資料可避免當設備故障或設備停產時，或設定轉換期與更換維護廠商時，降低影響機關業務運作的時間。

- 設備帳號權限清單

針對帳號權限的清單備份，以及防火牆連線紀錄的備份。

- 防火牆管理設定連線紀錄(含帳號與內容修改紀錄)

完整防火牆管理連線設定與修改紀錄，可與機關管理申請表比對，作為稽核的佐證資料。

- 防火牆管理規則 Deny log 紀錄

可記錄 Deny log，藉由檢查被阻擋的記錄，可以確認是否有應開通而未

開通的規則，且可藉由阻擋記錄判斷是否有惡意行為嘗試連線並預先做出反應措施。

3.1.7.5 網路設備定期設定備份檢核表

3.1.7.5.1 定期備份檢測

- 定期設定備份確認

是否定期備份處理，機關應訂立流程於固定時間進行備份。

- 具備 log server 收集重要網路設備資訊

確認是否有 log server 定期接收網路設備重要資訊。

- 備份資料中是否含管理登入登出資料

確認備份資訊中是否包含管理者的管理登入登出資料，以便能完整記錄機關管理者或是維護廠商登入重要核心設備的時間。

- 備份資料加註與安全保存檢測

- － 備份資料是否完成加註說明備份時間、備份人員與其他注意事項，以方便做後續使用。

- － 備份資料適當保護處理。

備份資料是否做適當保護處理，確保備份資料的安全性。

3.1.7.6 無線網路檢核項目

無線網路檢核項目請參考無線網路安全參考指引：

依據該指引針對「僅存取外網」、「可存取內外網」及「禁止使用」等 3 種情況執行檢核。

3.1.7.6.1 機關政策「僅存取外網」無線區域網路

針對政府機關開放民眾或辦公室人員僅用於連線至網際網路，此無線區域網路不可以存取至內網，因此其使用的安全防護機強調與內網的隔離性。

3.1.7.6.2 機關政策「可存取內外網」無線區域網路

針對政府機關開放辦公人員同時可以存取內網及網際網路資源，此無線區域網路因同時具備存取內與外網的功能，因此其使用的安全機制必須非常完整，並配合該指引內文所提供的改善程序，進行矯正或預防。若無線區域網路安全需要重新制定或升級，則可參考無線網路安全參考「3.1 規劃」重新進行管理循環，再依據「3.2 執行」強化無線區域網路安全之管理，且利用「3.3 檢查」與「3.4 行動」進行無線區域網路安全管理之調整與修改。

3.1.7.6.3 機關政策「禁止使用」無線區域網路

針對完全禁止使用無線區域網路的政府機關，主要是以控管與監測機關內的非法使用無線區域網路傳輸之行為，並輔以管理措施導入。

於以下章節中，如有需要，本指引將針對機關之「僅存取外網」、「可存取內外網」及「禁止使用」政策採取個別建議說明，反之，當內容中無特別註明適用何種政策，則表示採用 3 種政策之機關皆適用該段內容說明，機關可自行選擇參閱。

3.1.7.6.4 無線網路架構確認

- 提供無線網路架構圖具體現狀

是否具備無線網路邏輯與實體架構圖。

- 無線網路採中央集中管控

確認無線網路是否採中央集中管理以確認其安全性。

- 無線網路與有線網路採實體分隔

檢查無線網路是否與機關有線網路實體隔離以確保安全。

- 無線存取點樓層平面圖

是否具備無線存取點的樓層平面圖，方便管理者確認存取點實際位置。

3.1.7.6.5 無線網路管理狀態確認

- 無線網路認證管理方式確認。Web 或是 GUI，並採連線加密

確認無線網路控制器管理方式，同時檢查管理連線是否加密。

- 管理帳號權限確認

檢查管理帳號權限，確認是否符合機關管理原則，並且依據權限，不同管理者使用不同帳號。

- 僅允許特定 IP 執行管理設定

針對管理連線是否有限定管理來源 IP，以增加管理安全性。

- 管理設定不允許採遠端存取方式執行

是否有限制外部管理，避免由外部連線管理時衍生的風險，若需外部連線管理需搭配機關配套方式，例如透過 VPN 連線進入內網後再進行限制連線存取管理。

3.1.7.6.6 無線網路使用者存取確認

- 無線網路認證金鑰採用合宜加密方式

確認無線網路存取使用何種方式，是否符合安全需求。

- 無線網路服務集識別元(Service Set Identifier, SSID)已隱藏

確認無線網路內部使用 SSID 是否隱藏，外部訪客是否可以探察取得。

- 針對訪客與內部人員提供適當阻隔規則

確認無線網路管理是否適當阻隔內部使用與訪客的存取，確保機關資料使用安全。

- 使用者採多重認證技術

確認使用者除了金鑰之外，是否需透過身分認證(帳號密碼)，以增加無線管理的使用者存取安全性。

- 記錄無線使用者進出資訊

確認針對無線使用者的進出使用連線是否留存紀錄，有需要時可進行查詢，可針對特定時間內的使用者進行過濾與確認，查詢出對應的 IP 與 MAC 供資安需求單位用以反查。

3.2 「執行」

依據機關提供整體網路邏輯架構圖(包含資安設備如 IPS/IDS)、整體網路實體架構圖、系統連線邏輯架構圖、系統連線實體架構圖(包含所有經過的網路設備、線路)、系統連線防火牆規則(包含系統所在的網段、any source、any destination)與網路管理人員依據網路架構訪談，並討論檢核表內容與說明檢核表自評項目，機關可依據此方式執行。

3.2.1 執行導入前置需求

依據 3.1.1 規劃階段進行訪談與會議討論，會議說明 3.1.2 -3.2.6 的規劃歷程，解說檢核表與討論檢核內容與流程，確認導入範圍與導入時間規劃，請機關針對內部資料先行匯集，供後續檢核階段機關自評。

3.2.2 確認 IP 設定與區域劃分

機關可參考 3.1.2 規劃實際針對相關設備資料設定，設備 IP、網段劃分進行

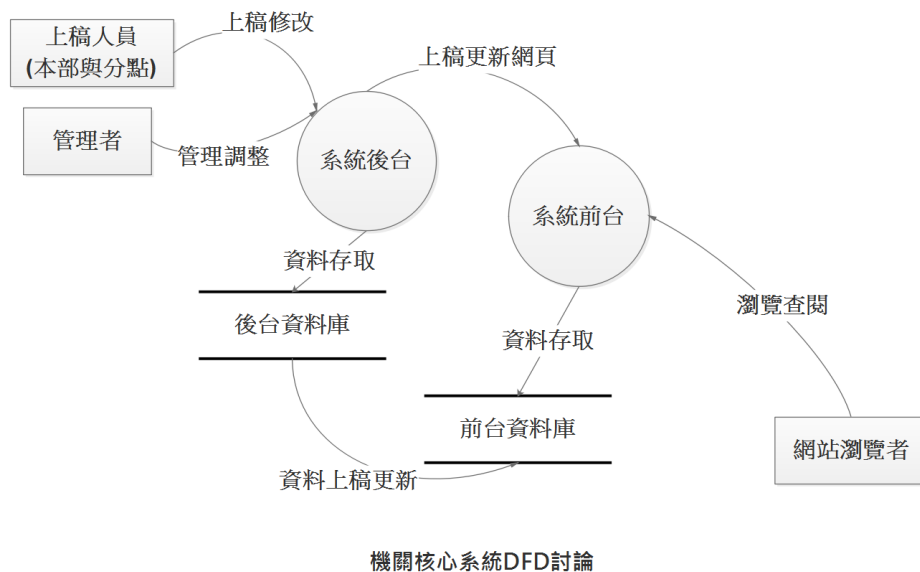
資料彙整，或依據機關現有的資料進行整理都後續執行階段使用。

3.2.3 確認 VLAN 與路由

機關可參考 3.1.3 規劃實際針對相關設備進行設定，透過設備 VLAN 劃分達成規劃需求。完成後進行路由設定，此階段通常需要外部相關機關或 GSN 配合施作，此部分在規劃階段應該調查好對應窗口與處理方式，路由劃分與設定會在完成 IP 設定區域劃分與 VLAN 切割之後實施。

3.2.4 確認機關資料流程圖繪製

依據 3.1.4 規劃繪製資料流程圖，主要是確認核心系統的資料流，同時藉由檢核結果了解實際運作現狀，判斷是否須調整優化流程或增加控制選項以加強安全性，繪製討論流程與結果詳如圖 27 所示。

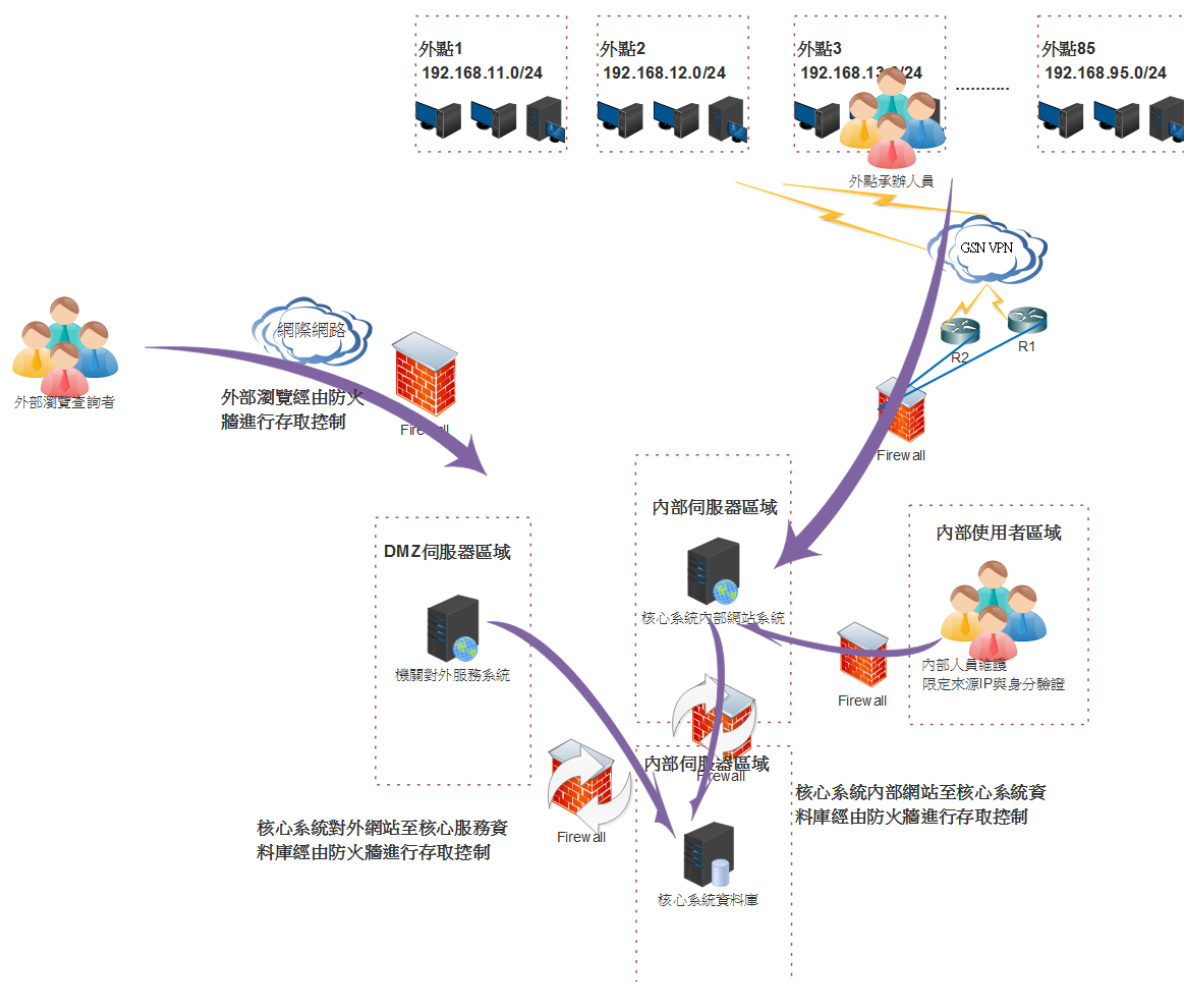


資料來源：本計畫整理

圖27 機關核心系統 DFD 繪製圖

3.2.5 確認區域間存取控制

機關可參考 3.1.5 規劃進行實作執行，須依循預先整理的存取控制列表建立，包含管理規則、順序、區域等設定，實務上存取控制可能設定於防火牆或是核心交換器上，在執行後應予以檢測確認管理規則的可用性與正確性，機關核心系統存取控制檢核詳如圖 28 所示。



資料來源：本計畫整理

圖28 機關核心系統存取控制檢核

3.2.6 執行查檢表比對機關資料

依據 3.1.7 規劃所整理的細項檢核表，針對機關實際執行建置後的網路與設備狀態進行檢測，確認執行的可用性與正確性。

3.3 「檢查」

網路架構查檢應定期審查，並列為內稽必要項目，分述如後：

3.3.1 檢查機關網路架構

在機關依據規劃執行建置完成機關網路後，應依據 3.1.7 規劃所整理的機關網路檢核表中的網路架構部分，針對已完成建置的架構進行比對確認，確認架構的正確性及完整性，並檢核架構是否有所遺漏或是有改善空間。

3.3.2 檢查區域分隔與存取控制

依據 3.1.7 規劃所整理的檢核表中防火牆檢核表(區域分隔與存取控制部分)，針對機關規劃建置的結果進行資料比對確認，檢測建置結果是否符合規劃方向與原則，同時也確認存取控制是否需要調整管理規則以符合實際運作階段機關需求。

3.3.3 檢查結果整理彙整

依據細項檢核表中查核結果進行分項彙整，條列檢查結果，作為專家顧問建議的依據，讓機關可以依據建議進行架構的調整與優化。

3.4 「行動」

3.4.1 矯正措施

依據檢核結果，進行細項分析，歸納機關中諸如架構誤植，設定錯誤或其他調整建議。

3.4.2 預防措施

針對檢核結果中未立即有風險或其他建議事項，提供建議，讓機關能夠進行預防措施防止可能衍生的問題。

4. 實務範例

4.1 實務範例(一)

經核定以 A 機關資訊單位做為本案之導入機關，辦理實務導入作業，導入結果，詳見附件 2 所示。

4.2 實務範例(二)

經核定以 B 機關資訊單位做為本案之導入機關，辦理實務導入作業，導入結果，詳見附件 3 所示。

5. 參考文獻

- [1]行政院國家資通安全會報，資通安全事件通報及應變辦法.，107 年版
- [2]NIST，Special Publication 800-53 Revision 4，Recommended Security Controls for Federal Information Systems，January 2014
- [3]NIST，Special Publication 800-77，Guide to Ipsec VPNs，December 2005
- [4]Diffie，W、Hellman，M(1976)「New directions in cryptography」IEEE Transaction on Information Theory，Vol IT-22，No. 6，pp644-654
- [5]Rivst，R； Shmir，A； Adleman L(Feb 1978)「A Method for Obtaining Digital Signatures and Public-Key Cryptosystems」Communication of the ACM，pp120-126
- [6]FIPS Pub 186-4：Digital Signature Standard(DSS)July 2013，csrc.nist.gov(pp 15-21)
- [7]IETF RFC 2104 HMAC
- [8]NIST SP 800-38A，「Recommendation for Block Cipher Modes of Operation」
- [9]FIPS PUB 197，Advanced Encryption Standard(AES)
- [10]NIST，「Recommended Elliptic Curves for Government Use」
- [11]103 年政府行動化安全防護規劃報告
- [12]https://en.wikipedia.org/wiki/Elliptic_curve

6. 網站資源表列

[1]行政院國家資通安全會報技術服務中心(<https://www.nccst.nat.gov.tw/>)

[2]NIST Special

Publication(<http://csrc.nist.gov/publications/nistpubs/index.html>)

[3]ISO Standard Catalog(<http://www.webstore.ansi.org/ansidocstore/>)

[4]TUV-IT ITBPM(<http://www.bsi.de/english/gshb/index.htm>)

7. 附件

附件1 「網路架構規劃」安全控制措施查檢表

附件2 機關導入完整報告(一)

附件3 機關導入完整報告(二)

附件4 專有名詞中英對照表

附件5 導引手冊 Quick Guide