

# 內容傳遞網路服務跨域技術之探討

曾惠敏

財團法人國家實驗研究  
院國家高速網路與計算  
中心

0303118@narlabs.org.tw

周大源

財團法人國家實驗研究  
院國家高速網路與計算  
中心

1203053@narlabs.org.tw

黃文源

財團法人國家實驗研究  
院國家高速網路與計算  
中心

wunyuan@narlabs.org.tw

胡乃元

財團法人國家實驗研究  
院國家高速網路與計算  
中心

2103081@narlabs.org.tw

劉德隆

財團法人國家實驗研究  
院國家高速網路與計算  
中心

tliu@narlabs.org.tw

## 摘要

國網中心已於111年度完成公共服務網路內容傳遞服務 (Content Delivery Network, CDN) 之建置, 將邊緣節點 (Edge) 佈署於台南與新竹兩地, 未來因應使用量成長所需, 以及當網站遭受 DDoS 攻擊或異常訪問量暴增造成負荷滿載, 除了進行邊緣節點的擴建外, 亦將尋求如教育部建置 CDN 服務間跨域之合作, 可促成跨域 CDN 的整合, 並建立有效的備援機制。本論文將依此需求, 探討各種跨域 CDN 之協同運作方式並進行驗證, 期能利用跨域之 CDN 資源啟動備援機制, 快速提供快取原網站之內容, 改善使用者瀏覽網站之整體效能, 藉以強化公部門服務網路之品質。

關鍵詞：傳遞網路、對等式內容傳遞網路、多內容傳遞網路

## I. 簡介

### A. CDN 背景

近年來愈來愈多客戶反應網站速度慢或遭受 DDoS 攻擊, 越來越多的企業使用內容傳遞服務 CDN 以減少對源站伺服器的請求, 可防止 DDoS 攻擊並提高效率。CDN 技術最早可追溯至1998年[1][2][3], 當時網站服務能力與網路頻寬均有限, 若透過反向代理 (reverse-proxy) 的機制, 可將網站內容快取到世界各地的快取伺服器, 再透過 DNS 或 anycast 路由等技術, 可將瀏覽對網站內容的請求動態配發到就近之快取伺服器, 如此將達到節省網路頻寬以及分散服務節點的效果。如圖1為 CDN 運作的示意圖, 左方為一般的服務架構, 來源網站需要面對所有使用者的流量, 因此網路頻寬與伺服器等級需依拜訪人數的成長而拓增, 同時亦須考慮資安防護等措施; 右方為採用 CDN 後之架構, 使用者的流量將被分散至各地的邊緣節點, 並由邊緣節點進行來源網站內容的快取, 可加速瀏覽速度並減少來源網站的負擔, 並協助進行資安過濾與防護。

CDN 服務應用於業界已經行之有年, 目前已經有許多企業皆有提供 CDN 網路服務, 如 Akamai[4]、Amazon[5]、Cloudflare[6]、中華電信[7]、CDNetworks[8]、Google Cloud CDN[9]等等。各家 CDN 供應商根據用戶地理位置、效能和成本管理有著不同的

路由政策和表現。各 CDN 供應商為用戶提供自身佈建的邊緣節點、底層網路基礎設施和資安防護功能。因此倘若可跨域使用多個 CDN 業者之服務, 將可提高網站存取效能、並增加其安全性和使用彈性, 但考慮各家 CDN 之服務無論建置設備、資安設備或監控系統, 以及管理維護流程等均各自為政, 如何整合各家 CDN 平臺以追求更加穩定之服務已是目前的熱門議題。

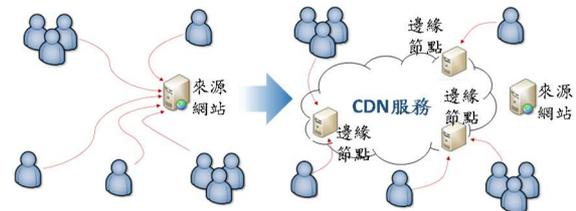


圖1. CDN 服務示意圖

### B. CDN 跨域技術

為探討多家 CDN 服務間進行服務之協同合作, IETF 於2003年成立 Content Distribution Internetworking (cdi) 工作小組[10], 並嘗試從要求路由 (request routing)、配發 (distribution) 與計價 (accounting) 等三個層面進行跨域機制之探討, 然而在產出三個 RFC 後, cdi 工作小組於2003年結束運作, 於2011年再次成立新的 Content Delivery Networks Interconnection (cdni) 工作小組 [11], 定義 CDN 服務彼此互為合作關係, 若對其他服務發出資源需求的 CDN 稱為上游 CDN (uCDN), 接收此需求的一方稱為下游 CDN (dCDN), cdni 嘗試制定兩者間傳遞的資料與技術等規格。

同時歐洲電信標準協會 ETSI 亦進行相關標準的制定, 並於2013年擬定跨 CDN (CDN Interconnection, CDNI) 架構之技術規格[12], 類似 IETF cdni 工作小組的合作模式, 於不同的 CDN 服務間定義出連結交換控制 (Interconnection Control Function, ICF)、要求與內容控制 (Request & Content Control Function, RCF)、以及內容派發控制 (Distribution of Content Control Function, DCF) 三個介面、CDN 業者可透過這些介面以對等 (Peer) 的方式與其他 CDN 服務互惠合作。

近年來針對對等式 CDN 架構有多項相關研究, R. Buyya 等人於[13]提出一套以服務導向架構 (Service-Oriented Architecture, SOA) 的 CDN 協同運作方式,

CDN業者可透過此架構分享資源，以提供符合用戶 QoS 與 SLA 協議之服務。A. Binder 與 I. Kotuliak 依據 ETSI CDNI 架構建構出測試平臺[14]，並開發 CDNI Adapter 作為各 CDN 間溝通的程式介面，除驗證 CDNI 架構的正確性外，亦可分析網站內容分享的生命周期。

然而在實務上，大型 CDN 業者於世界各地投入大量資源建置機房設備與網路頻寬，以拓展自身的資源為主要發展模式，而非考慮透過對等式 CDN 的運作與其他業者合作，因此上述標準與研究成果並未被業界實作與採用。但是各家 CDN 在不同地區的服務資源或時段優惠上各有所長，對網站管理者而言只能選取一家服務，就需要仔細分析各家 CDN 的優劣勢，不過由於業者除了計費標準外，通常不會提供網路架構與機房位置及頻寬等資訊，導致網路管理者無從判斷，促成近年來新型態多內容傳遞網路 (Multi-CDN) [15] 的商業模式。

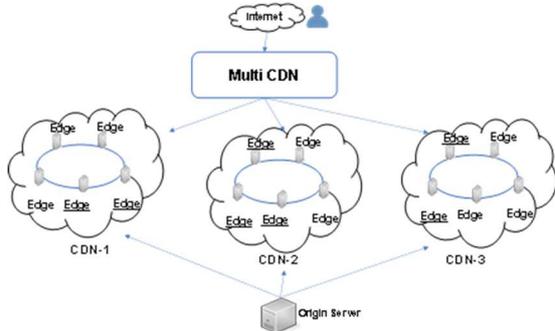


圖2. 多內容傳遞網路 Multi-CDN 架構

Multi-CDN 是指將眾家同 CDN 供應商的服務整合成單一系統，用戶只要透過 Multi-CDN 業者的介面即可設定與操作多個 CDN 服務，如“圖2”所示，來源網站向 Multi-CDN 供應商購買 CDN 服務，Multi-CDN 則預先訂閱多間下游 CDN 供應商 (CDN-1、CDN-2 與 CDN-3) 的服務，當使用者欲瀏覽來源網站時，會由 Multi-CDN 依不同的政策進行路由派發導向到最適當的下游 CDN，並由該 CDN 的邊緣節點協助來源網站的快取。因 CDN 各家供應商於各地的加速效果不一樣，若某企業需要購買多家 CDN 服務，透過 Multi-CDN 系統僅需做一次快取規則和資訊安全防護規則設定即可，不需逐一做個別設置，即可提供快速服務佈署、調度 CDN 彈性和可用性，為企業在不同的 CDN 線路間自動選擇最快網路路徑，並在發生故障時實現容錯機制。Multi-CDN 是一種結合不同 CDN 供應商的優勢，同時避免每個不同 CDN 供應商弱點的呈現。另一方面，使用者也無須進行大幅度變更和額外增加成本建置，即可增強其服務能量，提升網站的效能和穩定性。此方面亦有相關學術研究，在 [15] 中，S. Cui 等人於 Multi-CDN 架構中設計加密機制以保護用戶資料與使用偏好等隱私。O. Hohlfeld 等人則使用 Cedexis 的 Multi-CDN 服務進行各項數據的量測[16]。

### C. 國網中心 CDN 服務

國家高速網路與計算中心承接行政院國家發展委員會前瞻基礎建設計畫中第三期「強化公部門網路服務與運算雲端基礎設施計畫」，配合福爾摩沙開放網際網路交換中心 (Formosa Open eXchange, FOX) 的建置，於台灣高品質學術研究網路 TWAREN (Taiwan Advanced Research and Education Network) 骨幹上構建 CDN 服務 [17]，可結合 TWAREN 骨幹網路與 FOX 交換中心的優勢，代理網站服務並快速將內容遞送到終端瀏覽者。相關開發與建置購案由敦陽公司得標，採用線上探索公司的 Aspirapps CDN 解決方案[18]，110年於台南分部建置實驗平臺進行驗證測試，111年完成 CDN 正式平臺的服務，並於新竹本部與台南分部佈署 CDN 邊緣節點，預計未來三年會逐年擴充1個節點，除了拓展系統服務量能，同時增加派發之彈性以有效分散網路流量，預計 112年可為政府公部門公共服務網站提供正式服務。由於教育部亦於此前瞻計畫中共同執行 TANet 上 CDN 服務之建置，為求雙方資源共享，我們也將以互惠原則共同規劃未來跨域 CDN 可行的合作模式。

### D. 資訊安全考量與規劃

因應網路新型態的威脅攻擊趨於多元，我們更須強化整體系統安全防護鍊的規劃，由於國網中心 CDN 使用 TWAREN 研究網路骨幹頻寬，並協助公共服務網站進行內容代理，資安威脅是無法避免的。在系統存取規劃部份，我們使用 SSLVPN 作為管理 CDN 系統與外部網路隔離及進入 CDN 系統之存取控制方式，確保只有維運相關人員可進入設定；為了防護外界對於 CDN 系統各種網站攻擊，我們於邊緣節點前建置應用程式防火牆 (Web Application Firewall, WAF)，針對常見的攻擊類型，如資料隱碼 (SQL injection) 攻擊與防禦、跨網站攻擊 (Cross Site Scripting, XSS) 與防禦、暴力攻擊 (Brute Force login) 與防禦、參數值之竄改 (Parameter Tampering) 攻擊與防禦、資訊外洩 (Information Leakage) 等進行防護；此外，當遭受分散式阻斷服務 DDoS 攻擊時，相關封包與流量會由 TWAREN 骨幹 DDoS 偵測與清洗中心進行協防，以維持網路正常運作；最後，為符合相關資安法遵，平台之建置皆符合資通系統普級資安需求項目，未來也將在各邊緣節點前端擴充次世代防火牆和入侵偵測系統，作為存取管控及阻擋惡意攻擊與漏洞，以強化安全防禦措施。

縱上所述，從技術面來看，對等式 CDN 是 Multi-CDN 的其中一種案例，因此我們將探討達成 Multi-CDN 所需之技術，並利用目前已建置完成的 CDN 實驗與正式平臺規劃出測試架構並進行概念驗證。本論文的組織架構如下：第2節介紹多內容傳遞網路 Multi-CDN 的運作策略與特性；第3節說明所提出的驗證架構與規劃；在第4節中展示驗證多內容傳遞網路切換技術的可行性並討論其結果；結論與未來展望將在第5節說明。

## II. 多內容傳遞網路 Multi-CDN 探討

對企業而言，希望能確保他們的網站能夠覆蓋整個地球上的每個用戶，因此盡可能選擇擁有最多的邊緣節點覆蓋率的 CDN 供應商，讓用戶減少網頁加載的時間，透過 Multi-CDN 架構，網頁、圖片、媒體影音服務等內容被暫存在不同地理區域的多個 CDN 供應商之間，將可比單一 CDN 供應商達到更佳的效果。由於各家 CDN 供應商的覆蓋範圍不同，有些在美洲有優越的覆蓋率，有些在亞洲有更好的覆蓋率，選擇將流量路由到不同的 CDN 上，可以在效能和可用性上達到最大的效益，故路由派發導向的選擇很重要，這也是 Multi-CDN 重要的核心技術。各家多內容傳遞網路 Multi-CDN 路由決策的標準各不相同，我們根據常見的切換技術歸納為無負載平衡設備與有負載平衡設備兩種[19][20][21]，分析探討如下：

### A. 無負載平衡設備

在無負載平衡設備的架構下，CDN 的派發導向主要以靜態 DNS CNAME 的設置方式為主，因為 DNS 的簡單性、控制性和易用性，在上游的 Multi-CDN 可以很容易地為每個下游 CDN 配置靜態 DNS 設定，例如，用戶可以將 A 網域流量導到 CDN-1，將 B 網域流量導到另一個 CDN-2，如果 CDN-1 故障欲將流量轉移到 CDN-2，只需透過簡單手動更改 DNS CNAME 記錄即可。雖然這種技術看起來很簡單，但缺點是 DNS 需要經過幾分鐘的擴散時間，也不會自動去對 CDN 作健康監控，由於過程中都是透過管理者監視與手動操作，除了需要較長的反應時間外，如果不小心設定不當會導致效能下降或造成服務的中斷。

### B. 有負載平衡設備

為了能夠持續提供不中斷的服務，Multi-CDN 在派發時通常會透過負載平衡設備，以防止下游單一 CDN 供應商的故障的風險，此部分依所使用的技術又可分為 DNS 負載平衡與 HTTP 導向兩種：

#### I. DNS 負載平衡

市面上的一些 DNS 負載平衡設備可支援用戶自定義流量的路由規則，當 Multi-CDN 訂閱了所有需要的下游 CDN 網路後，可以複製所有 CDN 網域並 CNAME 到 DNS 記錄中，並根據以下的幾種規則設定，當用戶請求 CDN 解析名稱時，依規則將最佳的 CDN 回應給用戶進行訪問的派發導向：

- 循環制 (Round-robin)：以輪詢的方式依次將流量平均分配到不同的 CDN。例如，在兩個 CDN 配置中，請求 1 到 CDN-1，請求 2 到 CDN-2，請求 3 轉到 CDN-1，並依此類推。

- 加權輪詢算法 (Weighted round-robin)：是另一種是加權輪詢的方式，用戶可以依據業務需求經由權重比例設置分配流量到指定的 CDN 上。例如，在 3 個 CDN 的多 CDN 線路中，可以將 60% 的流量分配到 CDN-1，30% 分配到 CDN-2，20% 分配到 CDN-3，此方法可提高快取命中率，同時在每個 CDN 之間區隔流量。
- 地理位置定位：根據使用者的地理位置來回應 CDN 服務，對於每個請求會 CNAME 至距離用戶最近的 CDN，如此一來特定區域內用戶的流量將會盡量導至該區域 CDN 供應商，較具有成本和效能的優勢。

#### II. HTTP 重新導向方式

市面上的一些 DNS 負載平衡設備可支援用戶自定義流量的路由規則，當 M 若採用 HTTP 重新導向的技術，當系統想要將流量從一個 CDN 轉移到另一個 CDN 時，負載平衡服務器會回應一個 HTTP 302 (Found) 狀態碼，告訴在該 CDN 網路上請求回應標頭指示到另一個備用 CDN 網路，通常會給瀏覽器傳送 HTTP Location 標頭來重新導向到新的位置。與 DNS 切換相比，HTTP 重定導向可以更快地回應用戶請求，但瀏覽者在網址列上看到的將是導向後的網址而非原站網址。

### C. 負載平衡設備政策考量

雖然使用上述負載平衡設備是目前大多數企業最簡單的選擇方法，但是仍需要透過不同平臺單獨訂閱和管理各項 CDN 服務，當然 Multi-CDN 除了負載平衡調配服務外，還需要加上自動監控機制，經由實際量測 CDN 品質、網路延遲數據和客戶端遙測，依據量測結果智慧化地調度目前狀態最佳的 CDN 服務，相關需考慮負載平衡的因素如下：

- CDN 服務成本：不同的 CDN 供應商針對不同地理位置，高峰與非高峰時段、批發定價等有不同的定價管理成本。
- CDN 邊緣節點效能：每個 CDN 供應商運行邊緣節點方式不同，可能使用不同的上游網際網路服務供應商 ISP 網路，不同 CDN 供應商營運的邊緣節點因地理位置也具有不同的延遲和加速效果。
- CDN 擴展性和可用性：雖然 CDN 供應商都運行在大型商業網路上，但頻寬非無限容量，在流量高峰時可能會造成負荷過載，而區域性中斷時也可將流量轉移選擇其他路由，避免單點故障中斷服務。
- CDN 安全性：針對 DDoS 攻擊，CDN 業者可靠遍佈世界的邊緣節點分稀釋 DDoS 的封包，此外也可購買商用或自建流量清洗服務，透過分析骨幹封包的 NetFlow 或 sFlow 偵測可能的 DDoS 攻擊，再以 BGP FlowSpec 將帶有攻擊的封包導向 DDoS 清洗中心，清洗後將乾淨的封包送回原目的地，因此各 CDN 業

者本身已具備 DDoS 防護能力，在擁有多個 CDN 供應商狀況下更可以降低 DDOS 風險，攻擊者不太可能同時摧毀兩個或多個的 CDN 供應商，不至於造成全部的網路癱瘓。

此外，由於多內容傳遞網路因來自不同供應商的 CDN 網路，應該避免使用相同上游網路和相同數據中心的 CDN 供應商，且選擇雙重或多重 CDN 策略，以防止單一供應商的故障的風險，避免影響業務中斷提升服務可靠性，同時針對不同狀況、時間段和地理位置，以及考量不同 CDN 供應商之間的商業競爭價差來強化服務能量，達到成本的控制目的。瞭解上述實現多內容傳遞網路服務的不同配發技術和服務特性得知，Multi-CDN 要選擇出最合適的 CDN 和網站效能最佳化，除了切換技術、預算和 CDN 規模外，需要有多重的組合方式需要分析考量。

### III. 系統架構

在本節中，我們以 DNS 負載設備之技術為依據，對目前國網中心所建置的 CDN 正式與實驗平臺間之服務備援進行相關可行系統架構之規劃，在此情境下 CDN DNS 派發系統扮演重要的角色，透過 CDN DNS 派發系統由原站 DNS 將原站之網址以 CNAME 紀錄方式轉址至 CDN DNS 網域，並依所對應之政策，回覆適當之 CDN 邊緣節點 IP 位址或再 CNAME 至下游之 CDN。藉由此技術模擬跨域 CDN 平臺間之合作模式，互相作為後續維運期間的備援平臺，以改善瀏覽用戶的使用體驗。我們採用下列兩種合作模式之情境，分別為階層式內容傳遞網路和對等式內容傳遞網路，各架構運作原理將分別於子章節列述。

#### A. 階層式內容傳遞網路

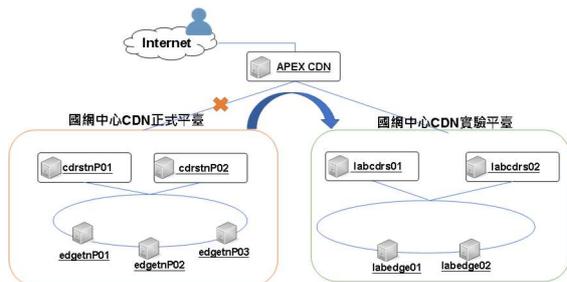


圖3. 階層式內容傳遞網路

在如“圖3”的階層式架構中，會由一個最上層的 CDN 服務 (APEX CDN) 以單一管理平臺負責統籌協調派發工作，結合國網中心正式與實驗平臺的現有 CDN 資源，負責同步管理兩個 CDN 平臺提供服務與備援機制，依各自 CDN DNS 派發系統的路由政策設定，根據用戶位置執行導向最近的邊緣節點，提供最佳化的資料傳輸服務，這裡的 APEX CDN 的 DNS 派發系統形同 Multi-CDN 供應商的扮演的角色，正式與實驗平臺則為

下游 CDN 供應商。

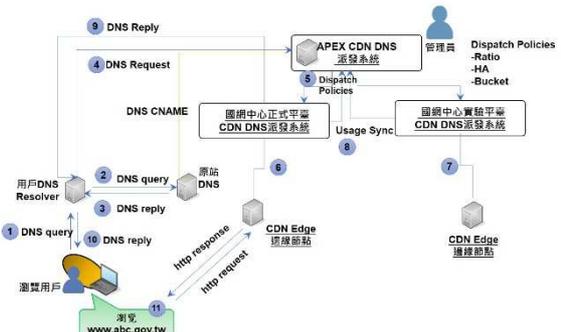


圖4. 階層式內容傳遞網路運作模式

在使用階層式 CDN 內容傳遞網路服務的情境中，假設網站 www.abc.gov.tw 主要是由 CDN 正式平臺進行服務，若正式平臺發生障礙則由實驗平臺接手服務，相關流程如“圖4”所示並說明如下：

(1) 用戶端由網頁瀏覽器瀏覽 http://www.abc.gov.tw 網站，(abc.gov.tw 域名需事先 CNAME 至 APEX CDN DNS)，用戶端裝置會向用戶端網域所在的 DNS Resolver 發出 DNS query 的請求。

(2)~(3) 瀏覽器第一次查詢發現本地端 DNS Resolver 沒有 DNS 暫存紀錄，轉向原站的 DNS 伺服器請求 DNSquery，原站 DNS 將 APEX CDN DNS 的 CNAME 紀錄回應至本地端 DNS Resolver。

(4)~(5) 本地端 DNS 向 APEX CDN DNS 派發系統作 DNS Request，APEX CDN DNS 將依據派發政策，預設 CNAME 至正式平臺，倘若正式平臺故障則 CNAME 至實驗平臺的 CDN DNS 進行詢問，在本情境中 APEX 將查詢 CNAME 至正式平臺。

(6)~(8) 正式與實驗平臺分別透過 API 將使用量與健康度等資訊同步至 APEX CDN DNS 系統。

(9)~(10) 由正式平臺將最適合的 CDN 邊緣節點 IP 位址回應給本地端 DNS Resolver，本地端 DNS Resolver 再將此解析的資訊回應給用戶。

(11) 用戶根據回應的 CDN 邊緣節點位址向正式平臺節點發出 HTTP Request 並獲取 HTTP Response。

#### B. 對等式內容傳遞網路

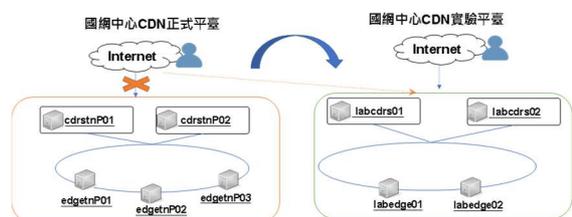


圖5. 對等式內容傳遞網路

在對等式 CDN 架構中，無需上層 APEX CDN 而是正式與實驗兩 CDN 平臺互相對等運作如“圖5”，對正式平臺而言，其 CDN 設定資料會預先預載在實驗平臺 CDN

DNS 派發系統上，當正式平臺 CDN DNS 派發系統判斷其下的邊緣節點無法提供服務需啟動調度使用時，會將原站 DNS 再次 CNAME 指向實驗平臺 CDN DNS 派發系統位址，屆時由實驗平臺 CDN DNS 派發系統將使用者瀏覽網頁的需求連線派發到旗下納管的邊緣節點接手分擔流量；反之對實驗平臺亦然，轉移過程中原站和網頁瀏覽使用者皆無須修改任何設定。在此情境下正式平臺和實驗平臺的 CDN DNS 派發系統都同時兼具上游 Multi-CDN 與下游 CDN 供應商的身分。

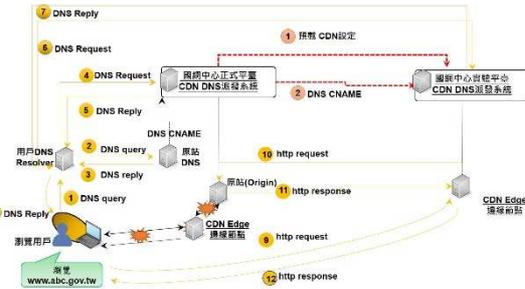


圖6.對等式內容傳遞網路運作模式

在此對等式的情境下，我們與前一小節相同地假設網站 www.abc.gov.tw 主要是由 CDN 正式平臺進行服務，若正式平臺發生障礙則由實驗平臺接手服務，相關流程如“圖6”所示並說明如下：

- (1) 用戶端由網頁瀏覽器瀏覽 http://www.abc.gov.tw 域名，(abc.gov.tw 的 CDN 資訊需事先 CNAME 至正式平臺 CDN DNS)，用戶端裝置會向用戶端網域所在的 DNS Resolver 發出 DNS query 的請求。
- (2)~(3) 瀏覽器第一次查詢發現本地端 DNS Resolver 沒有 DNS 暫存紀錄，轉向原站的 DNS 伺服器請求 DNS query，原站 DNS 將正式平臺 CDN DNS 的 CNAME 紀錄回應至本地端 DNS Resolver。
- (4)~(5) 本地端 DNS 向正式平臺 CDN DNS 派發系統作 DNS Request，此時正式平臺已偵測到其下邊緣節點已無法提供服務，故將實驗平臺 CDN DNS 派發系統位址回應給本地端 DNS Resolver。
- (6)~(8) 本地端 DNS Resolver 再向實驗平臺 CDN DNS 派發系統做 DNS Request，實驗平臺 CDN DNS 透過派發政策回應最佳的 CDN 邊緣節點 IP 位址回應給本地端 DNS Resolver，最終將此解析資訊回應給用戶。
- (9)~(12) 用戶根據回應的 CDN 邊緣節點位址發出 HTTP Request，由於是第一次訪問，邊緣伺服器會先向原站 HTTP Request，在獲取 HTTP Response 後回覆給用戶。

#### IV. 概念驗證

在探討國網中心的正式與實驗平臺兩個 CDN 間之備援模式後，我們將於本章節中進一步進行切換技術的驗證，相關設定與測試參數詳列如“表 I”，實驗方式與結

果於下一小節詳述。

表 I 驗證測試之設定與實驗參數

CDN 正式平臺	於國網中心台南分部之正式平臺，網域名稱為 cdn.fox.net.tw。
CDN 實驗平臺	於國網中心台南分部之實驗平臺，網域名稱為 cdn.twaren.net。
APEX CDN	於台灣 AI 雲 TWCC 之 VM，網域名稱為 aspirapps.info。
來源網站	由協力廠商線上探索公司架設測試用網站 aspirapps.com。
測試方式與參數	在切換前後每120秒以 Google 8.8.8服務對來源網站進行 DNS 解析，分別進行30次，並統計平均回應時間。

#### A. 階層式內容傳遞網路驗證結果

```
<<< DIG 9.16.1-Ubuntu <<> www-info.aspirapps.com @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 41498
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;; www-info.aspirapps.com.      IN      A

;; ANSWER SECTION:
www-info.aspirapps.com. 60      IN      CNAME   www-infoaspirappscom.aspirapps.info.
www-infoaspirappscom.aspirapps.info. 5      IN      CNAME   www-cdn6aspirappscom.cdn.twaren.net.
www-cdn6aspirappscom.cdn.twaren.net. 60      IN      A       211.79.3
```

圖7.階層式架構切換前由實驗平臺提供服務

```
<<< DIG 9.16.1-Ubuntu <<> www-info.aspirapps.com @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 5416
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;; www-info.aspirapps.com.      IN      A

;; ANSWER SECTION:
www-info.aspirapps.com. 60      IN      CNAME   www-infoaspirappscom.aspirapps.info.
www-infoaspirappscom.aspirapps.info. 5      IN      CNAME   www-cdn6aspirappscom.cdn.fox.net.tw.
www-cdn6aspirappscom.cdn.fox.net.tw. 60      IN      A       211.79.35
```

圖8.階層式架構切換後由正式平臺提供服務

在階層式架構中，來源網站的 DNS 會將其設定 CNAME 至 APEX CDN 的 DNS，在正常狀況下 APEX CDN 將此網站 CNAME 至實驗平臺 CDN 的 DNS，以讓實驗平臺提供 CDN 服務，當實驗平臺滿載或故障時由 APEX CDN 進行切換，改將網站 CNAME 至正式平臺 CDN 的 DNS 以維持原站之服務。“圖7”和“圖8”為切換前後以 dig 指令查詢 DNS 解析之過程，可以看到切換前後分別由實驗平臺與正式平臺提供服務。在此架構下，APEX 為上游 CDN，實驗平臺與正式平臺為下游 CDN，量測每120秒透過 Google DNS 查詢回應時間各30次計算平均值，切換前為133.5ms，切換後為153.7ms。

階層式架構的優勢為透過 APEX CDN 與下游 CDN 溝通相關資源使用，可智慧化進行 CDN 的派發，以避免單一下游 CDN 資源耗盡；缺點則為在沒有快取的情況下，DNS 解析的查詢需要經過兩次 CNAME 的時間，且下游 CDN 需要額外將內部的資料向上游 APEX 揭露。

## B. 對等式內容傳遞網路驗證結果

```
<<> Dig 9.16.1-Ubuntu <<> www-cdn6.aspirapps.com @8.8.8.8
;; global options: +cmd
;; Got answer:
-->HEADER<<- opcode: QUERY, status: NOERROR, id: 46588
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 512
;; QUESTION SECTION:
;www-cdn6.aspirapps.com.
IN A

;; ANSWER SECTION:
www-cdn6.aspirapps.com. 60 IN CNAME www-cdn6aspirappscom.cdn.twaren.net.
www-cdn6aspirappscom.cdn.twaren.net. 60 IN A 211.79.3 實驗環境CDN
```

圖9.對等式架構切換前由實驗平臺提供服務

```
<<> Dig 9.16.1-Ubuntu <<> www-cdn6.aspirapps.com @8.8.8.8
;; global options: +cmd
;; Got answer:
-->HEADER<<- opcode: QUERY, status: NOERROR, id: 41926
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 512
;; QUESTION SECTION:
;www-cdn6.aspirapps.com.
IN A

;; ANSWER SECTION:
www-cdn6.aspirapps.com. 60 IN CNAME www-cdn6aspirappscom.cdn.twaren.net.
www-cdn6aspirappscom.cdn.twaren.net. 5 IN CNAME www-cdn6aspirappscom.cdn.fox.net.tw.
www-cdn6aspirappscom.cdn.fox.net.tw. 60 IN A 211.79.35 正式環境CDN
```

圖10.對等式架構切換後由正式平臺提供服務

在對等式架構中，來源網站的 DNS 會將其設定 CNAME 至實驗平臺的 DNS 以提供 CDN 服務，當實驗平臺發生滿載或故障時則由實驗平臺 DNS 進行切換，將網站再一次 CNAME 至正式平臺 CDN 並由其維持原站之服務。在“圖9”中，切換前由實驗平臺提供服務；手動切換後如“圖10”，查詢會先到實驗平臺，經由再一層 CNAME 至正式平臺。在此情境下，實驗平臺為上游 CDN，正式平臺為下游 CDN，量測每120秒透過 Google DNS 查詢回應時間各30次之平均值，切換前為93.1ms，切換後為153.7ms，差異約達50ms，可以看出切換前僅經過實驗平臺 CNAME，因此會比切換後實驗與正式平臺共 CNAME 兩次查詢的速度較快，但50ms 的差異在時間上不易被使用者感知，且只會於第一次查詢時有所影響，且快取到查詢伺服器或主機後則無需再次查詢。

對等式架構的優勢為各 CDN 均為獨立運作，無需揭露內部資訊，且若在正常無切換的狀況下 DNS 解析僅需 CNAME 一次；缺點則為切換的時機由各 CDN 自行判定，無法確認各 CDN 間資源的用量與均衡，且由於單一 CDN 需身兼上下游的角色，需要進行客制化開發。

## V. 結論與未來展望

本論文探討目前跨域 CDN 所用到的技術驗證，並於國網中心建置的正式與實驗 CDN 平臺上進行切換驗證測試，結果顯示不論是階層式或對等式架構均能順利切換，且 DNS 查詢時間的差異上不易為使用者感知，因此採用何種架構進行跨域 CDN 合作應回到政策面考量，

由兩種架構的優缺點中找出雙方可接受的方案，未來教育部 CDN 建置完成後我們也將與其進行相關討論，以求雙邊公共服務資源之整合與有效運用。

## 誌謝辭

感謝本中心 TWAREN 與 FOX 團隊配合提供 CDN 建置所需之網路架構，以及線上探索科技協助本論文驗證測試開發所需的客制化功能與架構配置。

## 參考文獻

- [1] A. Vakali and G. Pallis, “Content Delivery Networks: Status and Trends,” IEEE Internet Computing, IEEE Computer Society, pp. 68-74, November-December 2003.
- [2] M. Pathan and R. Buyya “A Taxonomy and Survey of Content Delivery Networks,” Grid Computing and Distributed Systems Laboratory, University of Melbourne, Technical Report, 2007.
- [3] B. Zolfaghari, et al., “Content Delivery Networks: State of the Art, Trends, and Future Roadmap,” ACM Computing Surveys, vol. 53, issue 2, April. 2020.
- [4] Akamai, website: <https://www.akamai.com/solutions/content-delivery-network/>.
- [5] Amazon CloudFront, website: <https://aws.amazon.com/tw/caching/cdn/>.
- [6] Cloudflare, website: <https://www.cloudflare.com/>.
- [7] 中華電信 CDN, website: <http://www.cdn.hinet.net/>.
- [8] CDNetworks, website: <https://www.cdnetworks.com/>.
- [9] Google Cloud CDN, website: <https://cloud.google.com/cdn/>.
- [10] Content Distribution Internetworking (cdi), website: <https://datatracker.ietf.org/wg/cdi/>.
- [11] Content Delivery Networks Interconnection (cdni) website: <https://datatracker.ietf.org/wg/cdni/>.
- [12] ETSI TS 182 032 - V1.1.1 - CDN Interconnection Architecture, website: [https://www.etsi.org/deliver/etsi\\_ts/182000\\_182099/182032/01.01.01\\_60/ts\\_182032v010101p.pdf](https://www.etsi.org/deliver/etsi_ts/182000_182099/182032/01.01.01_60/ts_182032v010101p.pdf).
- [13] R. Buyya, et al., “A Case for Peering of Content Delivery Networks,” IEEE Distributed Systems Online, vol. 7, issue: 10, October 2006.
- [14] A. Binder and I. Kotuliak “Content Delivery Network Interconnect: Practical Experience,” 11th IEEE International Conference on Emerging eLearning Technologies and Applications (ICETA 2013), pp. 29-33, October 2013.
- [15] S. Cui, et. al., “Multi-CDN: Towards Privacy in Content Delivery Networks,” IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 5, pp. 984-999. September/October 2020.
- [16] O. Hohlfeld, et al., “Characterizing a Meta-CDN,” Passive and Active Measurement Conference (PAM) 2018, pp 114-128, March 2018.
- [17] 周大源、黃文源、曾惠敏、胡乃元、劉德隆，「公共服務網路內容傳遞服務平臺之建置」，TANet2021論文集，臺中，2021年12月。
- [18] Aspirapps, website: <https://www.aspirapps.com/>.
- [19] What is Multi-CDN and How Does It Work? website: <https://ottverse.com/what-is-multi-cdn/>.
- [20] What is Multi CDN and why businesses are adopting it website: <https://www.mlytics.com/blog/what-is-multi-cdn-and-do-i-really-need-it/>.
- [21] WHAT IS MULTI-CDN? website: <https://www.stackpath.com/edge-academy/what-is-multi-cdn/>.