內容傳遞網路服務跨域技術之實測—以國網中心與 Cloudflare 為例

曾惠敏　周大源　胡乃元　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
{0303118, 1203053, 2503134, tlliu}@niar.org.tw

摘要

國網中心自110年度起進行完成公共服務網路內容傳遞服務（Content Delivery Network，CDN）之建置，目前已佈署邊緣節點（Edge）於臺南、臺中、新竹、臺北等地，可有效將瀏覽封包依來源或系統負載分散至各節點，除了撙節網路頻寬，亦能協防原始網站的資安防護。然而為了提升服務的韌性，與其他 CDN 系統的跨域合作將是未來努力的方向，我們之前已針對各種跨域 CDN 技術進行探討，本年度與國際 CDN 業者 CloudFlare 共同合作實測，針對 Multi CDN 分流機制進行驗證，測試不同地理位置的用戶能否正確導向至國網中心 CDN 與 Cloudflare CDN。結果顯示，在各情境下能依照地理位置將流量正確分派，提升使用者存取效率。

關鍵詞：內容傳遞網路、多內容傳遞網路、DNS 延伸安全協定。

Abstract

Since 2021, the National Center for High-Performance Computing (NCHC) has completed the infrastructure of Content Delivery Network (CDN). Several edge nodes have been deployed in Tainan, Taichung, Hsinchu, and Taipei, which could effectively distribute browsing traffic into different edges according browser location or system load. The CDN System not only conserves backbone bandwidth but also helps enhance cybersecurity protection for the origin websites. To further improve service resilience, collaboration with other CDN systems will be a key direction moving forward. We have explored various Multi-CDN technologies in our past study, and this year we collaborated with the international CDN provider Cloudflare for joint testing. The verification focused on Multi-CDN traffic distribution mechanisms, testing whether users in different geographic locations could be correctly directed to either NCHC's CDN or Cloudflare's CDN. The results show that traffic are successfully transmitted under different scenarios, thereby improving user access efficiency.

Keywords: Content Delivery Network(CDN), Multi-CDN, Extension Mechanisms for DNS (EDNS).

1. 前言

1.1　內容傳遞網路 CDN 簡介

隨著網際網路多媒體服務的普及，如何有效率地將大量內容傳遞至全球用戶已成為關鍵議題。內容傳遞網路 CDN 應運而生，其核心理念為透過分散式節點與快取技術，降低原始網站伺服器負載，並縮短用戶端的存取延遲[1][2][3]。CDN 基本運作方式是於網路骨幹上部署多個邊緣快取節點，將熱門內容複製並分散儲存。當瀏覽者發送請求時，系統會根據 DNS 導向或 Anycast 技術，將請求導引至距離最近或負載最佳的節點，以加速回應，此外 CDN 亦提供分散式阻斷服務 DDoS 防禦以及應用程式防火牆（Web Application Firewall, WAF）等資安加值服務，保障原站與內容之安全。

1.2　國網中心 CDN 服務

國家高速網路與計算中心執行國家前瞻基礎建設計畫中「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）骨幹上建置 CDN 服務[4]，可透過 TWAREN 網路及 FOX 交換中心與各 ISP 直接互連的優勢，快速將內容遞送到終端瀏覽者。本購案由敦陽公司得標，採用線上探索公司的 Aspirapps CDN 解決方案[5]，部署架構如圖1，110年於台南分部建置實驗平臺，並在111~113年完成 CDN 正式平臺的服務，將 CDN 邊緣節點佈署於臺南、臺中、新竹與臺北三峽，預計114年底前於中研院建置最後一個節點，將服務擴散至臺灣北中南各地，增加派發之彈性以有效分散網路流量。目前已提供正式服務，對象為政府公部門或法人等具公共服務性質之網站，未來將規劃計價機制，並於正式收費後開放一般網站申請本服務。

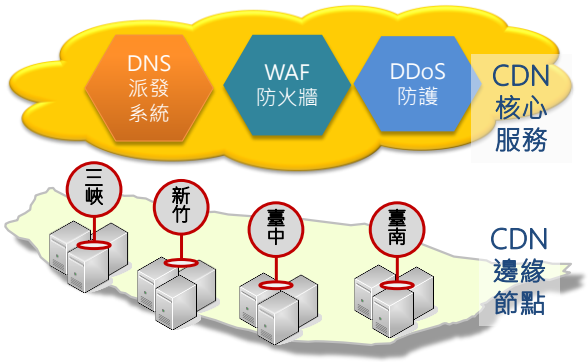

圖 1 國網中心 CDN 服務

1.3 多內容傳遞網路 Multi-CDN 架構

為了考慮單一 CDN 業者系統受阻礙時影響服務，網際網路工程任務組 IETF 及歐洲電信標準協會 ETSI 分別於2003及2013年成立 Content Distribution Internetworking（cdi）工作小組[6]及制定跨 CDN（CDN Interconnection，CDNI）架構[7]之技術規格，企圖讓不同 CDN 業者間透過標準介面可彼此支援，以提升系統穩定性並促進新服務之可能，我們於先前之研究中已有探討[8]，此種對等式 CDN 的優勢為各 CDN 均為獨立運作，主要的缺點則為 CDN 間需要協調彼此溝通所使用的標準並進行大量的客制化開發與設定。

然而在實務上各 CDN 業者各自有不同的收費機制及服務架構，難以透過對等方式跨 CDN 間彼此運作，因此促成近年來新型態多內容傳遞網路（Multi-CDN）的商業模式[9][10]。Multi-CDN 為階層式整合不同 CDN 供應商的服務成單一系統，讓用戶只要透過 Multi-CDN 提供介面可設定與操作多個 CDN 服務，其優勢為透過業者所架設之最高層的根 CDN（APEX CDN），針對各 CDN 業者的流量與收費等機制依使用者需求進行智慧化派發，缺點則為在沒有快取的情況下，DNS 解析需要經過 APEX CDN 與實際 CDN 服務業者兩次查詢的時間，但一旦 DNS 解析完成後在快取到期前將不會再次花費此查詢時間。

1.4 DNS 延伸安全協定（Extension Mechanisms for DNS，EDNS）及 EDNS 客戶子網域（EDNS Client Subnet，ECS）

隨著網際網路使用需求日益增加，傳統 DNS 協定逐漸受限於其在封包長度與功能擴充上的限制，為解決此問題，IETF 提出了 DNS 延伸安全協定（Extension Mechanisms for DNS，EDNS）[11][12]，允許在不改變 DNS 協定基本結構的情況下進行功能延伸。其中 EDNS 客戶子網域（EDNS Client Subnet，ECS）[13]是一項重要的擴充功能，能夠將使用者 IP 位址的部分資訊傳遞給上游 DNS 伺服器，以改善 CDN (Content Delivery Network) 與地理導向服務的正確性。

傳統 DNS 解析時，上游伺服器僅能得知遞迴解析器（Recursive Resolver）的 IP 位址，無法得知最終用戶的實際來源。因此，對於需要進行地理位置導向的 CDN 或負載平衡機制，可能會導致解析結果不精準。ECS 的設計目的即是將使用者 IP 位址的部分前綴（Prefix）傳遞給上游 DNS 伺服器，使其能根據用戶實際地理區域，回應最適合的伺服器 IP。

由於網域名稱系統安全擴充 Domain Name System Security Extensions，DNSSEC）需要啟用 EDNS 方能運作，為了確保 DNS 的安全性，自從2019年後各大 DNS 服務逐漸移轉並啟用 EDNS，但 ECS 是否支援仍視各 DNS 業者政策，部份 DNS 業者視 ECS 為網際網路的必要功能之一；而亦有 DNS 業者以用戶隱私為由不支援 ECS 的資訊傳遞。

1.5 小結

Multi-CDN 的派發機制主要將依瀏覽客戶的位置，配合流量、部署架構及收費標準等政策選取該地最適合的 CDN 業者，因此如何定位用戶為重要的核心技術。瀏覽客戶係透過 DNS 遞迴解析器發出 DNS 解析要求，因此 APEX CDN 將可由 DNS 解析器的 IP 位置判斷用戶所在地，當用戶使用其 ISP 提供的 DNS 解析器時判斷的細緻度將可到此 ISP 註冊的所在地，如教育部的用戶會設定所在區網中心的 DNS 解析器，APEX CDN 即可判斷其所在的區網中心；然而由於目前有眾多公用 DNS 解析器服務如中華電信、Google 與 Cloudflare 等可選取，倘若用戶透過這些公用 DNS 解析器進行 DNS 查詢，APEX CDN 將僅能透過 ECS 得知用戶真正的地區，但並非各個公用 DNS 解析器均支援 ECS，本論文將以國網中心與 CloudFlare 間的 CDN 派發為例，實測透過各個公用 DNS 解析器是否可讓 APEX CDN 依地理位置正確導向用戶至適合的 DNS 服務。在第2節我們介紹實驗之測試架構；第3節整理各情境下之測試結果；結論與未來展望將在第4節說明。

2. 實驗目的與架構

現今國網中心 CDN 邊緣節點均建置於 TWAREN 骨幹上，因此派發政策上僅能針對國內用戶的地理位置或所使用 ISP 進行最佳選擇；對國外的瀏覽者而言，由於封包均須送回國內節點，因此優化之空間受限。為此，我們與國際 CDN 業者 Cloudflare[14]進行合作，透過 Multi-CDN 架構辨識國內外的用戶以分別派發至國網中心或 Cloudflare 的節點，架構詳述如下。

此論文執行測試主要目的是為了驗證 Multi CDN 的分流機制是否可以依照用戶端地理位置正確地將流量導向指定的 CDN 節點，臺灣用戶透過國網中心 CDN 節點存取，而國外用戶使用 Cloudflare CDN 節點存取，測試過程中將記錄預期與實際導向的 CDN 節點提供服務是否一致。在如圖2的架構中，會由最上層的 APEX CDN 服務以單一管理平臺負責統籌協調派發工作，結合國網中心與 CloudFlare CDN 資源，負責同步管理兩個 CDN 平臺提供服務，

依 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。

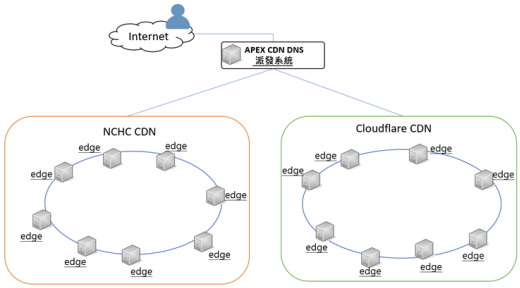

圖 2 跨國網中心與 Cloudflare 之 Multi-CDN 測試架構

在此測試情境下 CDN DNS 派發系統扮演重要的角色，首先原站 DNS 需將原站之網域以 CNAME 紀錄方式轉址至 CDN DNS 派發系統，CDN DNS 派發系統會依所對應之地理 IP 政策，回覆指派適當之 CDN 邊緣節點 IP 位址。我們藉此模擬跨域 CDN 平臺間之合作模式，可供未來國網中心 CDN 服務維運的參考，以改善瀏覽用戶的使用體驗。測試流程如圖3所示，當台灣用戶端查詢域名為 www-nchc.aspirapps.com 時，從查詢資料回應會看到 CNAME 至 Multi CDN DNS(APEX CDN DNS)主機 www.mcdn.aspirapps.net，Multi CDN 再依據用戶所在的位置來源導向指定的 NCHC 的 CDN 節點，反之，若國外用戶查詢域名為 www-nchc.aspirapps.com 時，Multi CDN 依據用戶所在的位置來源導向指定的 Cloudflare CDN 節點，詳細查詢流程如下述：

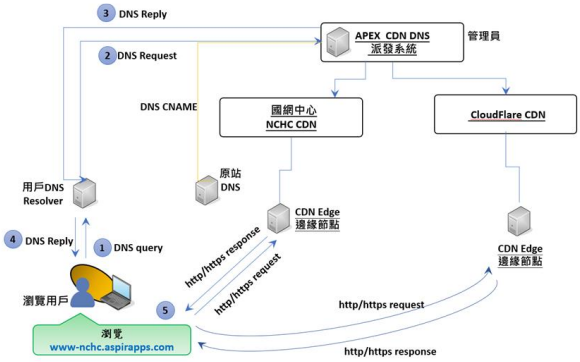

圖 3 Multi-CDN 測試流程

(1)用戶端由網頁瀏覽器瀏覽 http:// www-nchc.aspirapps.com 網站，(www-nchc.aspirapps.com 域名須事先 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。若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 APEX CDN DNS 的 CNAME 紀錄回應至本地端 DNS Resolver。

(2)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，回覆 CNAME 至 www.mcdn.aspirapps.net。

(3)~(4) 由 APEX CDN DNS 派發系統將最適合的 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。

(5)用戶根據回應的 CDN 邊緣節點位址向國網中心 CDN 節點或是 CloudFlare CDN 節點發出 HTTP Request 並獲取 HTTP Response。

如第一節所述，在步驟(2)中本地端 DNS 向 APEX DNS 發出請求時，APEX DNS 是否可判斷出瀏覽用戶的所在地將是正確派發的關鍵，為此我們將於下一節中針對國內用戶使用不同公共服務 DNS 的情境以及透過 VPN 使用模擬國外用戶進行實測並整理結果。

3. 測試方法與結果

3.1 測試配置與方法

接下來我們將進一步進行 DNS 分配的驗證，相關設定與測試參數詳列如表1。

表 1 驗證測試之設定與實驗參數

NCHC CDN	於國網中心台南部之正式平臺，(www-nchcaspirappscom.cdn.fox.net.tw)。
CloudFlare CDN	於 CloudFlare 之測試平臺，(www-nchcaspirappscom.cdn.cloudflare.net)。
APEX CDN	於台灣 AI 雲 TWCC 之 VM，網域名稱為 www.mcdn.aspirapps.net。
來源網站	由協力廠商線上探索公司架設測試用網站 www-nchc.aspirapps.com。
測試方式與參數	對來源網站進行 DNS 解析，分別進行100次，確認是否回傳支援 ECS（EDNS Client Subnet）之信息，並統計回應查詢結果。
國內測試網路	中華電信、台灣大哥大。
國內 IP 使用之公共 DNS	Google DNS (8.8.8.8) Hinet DNS (168.95.1.1) Cloudflare DNS (1.1.1.1) IBM DNS (9.9.9.11)
國外 VPN	日本、美國。
國外 IP 測試	透過 VPN 所取得之 DNS

使用 DNS	

我們將針對以上國內外情境使用 dig 或 nslookup 命令執行 DNS 查詢，並記錄返回的結果，於國內的網路中，我們分別設定 Google、Hinet、Cloudflare 與 IBM 的公共 DNS 確認是否支援 ECS 訊息，以及倘若不支援 APEX CDN 的判斷方式；國外的網路由於是透過 VPN 取得，只能使用 VPN 派發之當地 DNS。

3.2 系統設置與驗證步驟

3.2.1 Multi CDN 設置

如圖4及圖5所示，首先於 APEX CDN 中新增兩個下游 NCHC CDN 以及 Cloudflare CDN，接著設定 Multi CDN 派發規則：台灣用戶使用 NCHC CDN，非台灣用戶使用 Cloudflare CDN。

圖 4 APEX 下游 CDN 設定

圖 5 APEX CDN 派發機制設定

3.2.2 本機設定 DNS

改本地裝置的 DNS 設置，依序切換到8.8.8.8或其他測試用 DNS 等。。

3.2.3 本機執行 DNS 查詢

使用 nslookup 命令依序進行各 DNS 查詢，如：nslookup www-nchc.aspirapps.com 8.8.8.8。

3.2.4 記錄結果

查詢100次（每次查詢皆須清除 DNS 快取）紀錄返回的 CNAME 或 IP 地址，並核對是否與預期的 CDN 節點相符。

3.3 驗證測試結果

3.3.1 中華電信

表2為使用中華電信 IP 211.75.X.36分別透過 Google、Hinet、Cloudflare 及 IBM 查詢的結果，於 APEX CDN 上觀察發現只有 IBM DNS 支援 ECS 資訊，雖然其他 DNS 不支援 ECS，但由於透過 Anycast 找到最近的 DNS 解析器均位於國內，因此 APEX CDN 仍會正確地派發給國網中心的 CDN；此外我們亦觀察到 IBM DNS 應該於國內沒有代理伺服器，因此 APEX CDN 看到其查詢的 IP 來源為香港，然由於 IBM DNS 有將 ECS 211.75.X.0/24資訊傳送給 APEX CDN，因此我們能正確地派發給國網中心 CDN。

表 2 中華電信實測結果

用戶 IP	使用 DNS	是否支援 ECS	公共 DNS 查詢 IP 之所在地	ECS 資訊	派發是否正確
211.75.X.36	Google	否	臺灣	無	是
	Hinet	否	臺灣	無	是
	Cloudflare	否	臺灣	無	是
	IBM	是	香港	211.75.X.0/24	是

3.3.2 台灣大哥大

表3為使用台灣大哥大 IP 101.9.Y.216分別透過 Google、Hinet、Cloudflare 及 IBM 查詢的結果，和上一小節相同，APEX DNS 均能正確的派發到國網中心的 CDN 系統，唯一不同點是台灣大哥大是透過 IBM 在美國的 DNS 解析器向 APEX CDN 發出請求，但仍不影響派發之結果。

表 3 台灣大哥大實測結果

用戶 IP	使用 DNS	是否支援 ECS	公共 DNS 查詢 IP 之所在地	ECS 資訊	派發是否正確
101.9.Y.216	Google	否	臺灣	無	是
	Hinet	否	臺灣	無	是
	Cloudflare	否	臺灣	無	是
	IBM	是	美國	101.9.Y.0/24	是

3.3.3 國外 VPN（日本及美國）

我們接著透過 VPN 取得日本與美國的 IP

為203.10.M.164及185.205.N.187，由於透過VPN業者於國外當地的DNS進行查詢，APEX CDN均能正確判斷需派發給Cloudflare CDN。

表 4 日本 IP 實測結果

用戶 IP	使用 DNS	是否支援 ECS	公共 DNS 查詢 IP 之所在地	ECS 資訊	派發是否正確
203.10.M.164	透過 VPN 所取得之 DNS	否	日本	無	是

表 5 美國 IP 實測結果

用戶 IP	使用 DNS	是否支援 ECS	公共 DNS 查詢 IP 之所在地	ECS 資訊	派發是否正確
185.205.N.187	透過 VPN 所取得之 DNS	否	美國	無	是

4. 結論

在針對台灣用戶進行的測試中，包含中華電信與台灣大哥大使用各家公共DNS伺服器均能將請求正確導向國網中心CDN節點。在針對國外用戶日本與美國的網路測試中，請求均導向Cloudflare CDN，與預期結果完全一致。APEX CDN主要依靠然而各家公共DNS服務所傳遞的ECS資訊判斷來源用戶的所在地，但經驗證僅IBM DNS支援ECS，而其它公共DNS因在臺灣有設置伺服器因此APEX CDN仍能正確派發，但倘若用戶使用不支援ECS且在臺灣無DNS代理伺服器之服務將會被誤判成國外用戶，因此此派發機制無法保證完成正確。且此情境為以國內外來源區分國網中心與Cloudflare CDN，倘若是國網中心與教育部CDN之分流，假使用戶使用不支援ECS的公用DNS將無法正確判斷來源IP是否來自於TANet或其他ISP，影響APEX之派發依據。

綜上所述，我們已驗證國網中心若與Cloudflare合作將國內外分流之可行性，雖然以現有的機制無法達到完全正確之保證，但以測試的項目均通過驗證，為了服務之穩定及韌性，Multi-CDN仍是現階段可考慮採用之分流技術。

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] 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。

[5] Aspirapps, website: https://www.aspirapps.com/.

[6] Content Distribution Internetworking (cdi), website: https://datatracker.ietf.org/wg/cdi/.

[7] 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.

[8] 曾惠敏、周大源、胡乃元、劉德隆，「內容傳遞網路服務跨域技術之探討」，TANet2022 論文集，臺中，台灣, 2022 年 10 月。

[9] O. Hohlfeld, et al., “Characterizing a Meta-CDN,” Passive and Active Measurement Conference (PAM) 2018, pp 114-128, March 2018.

[10] 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.

[11] Vixie, P., et al., Extension Mechanisms for DNS (EDNS0). RFC 2671, 1999

[12] Damas, J., Graff, M., & Vixie, P., Extension Mechanisms for DNS (EDNS(0)). RFC 6891. 2013.

[13] Contavalli, C., van der Gaast, W., Lawrence, D., & Kumari, W., Client Subnet in DNS Queries. RFC 7871, 2016.

[14] Cloudflare, website: https://www.cloudflare.com/.