Soar with the Combined Strength of Multiple Clouds - Building Inter-Cloud Environment among TWCC, CCX and AWS

陳敏　古立其　李慧蘭　林書呈　謝學維　楊哲男
財團法人國家實驗研究院國家高速網路與計算中心
{minchen, lku, gracelee, daniellin, 1203039, yangcn}@narlabs.org.tw

摘要

自行購置硬體建置所需的計算環境，受經濟規模小、利用率低、且管理成本高所限，早已難敵雲端計算的浪潮。但不同雲端平台的特性各有所長，加上法規或機敏性的限制，並非所有的資料都適合擺在國外商業雲端環境中。因此若能結合不同雲端平台之長，或以自有設施結合雲端資源形成混合雲，便能在功能、節費、或敏感資料維護上得到最佳平衡。但打通不同雲平台卻難以避免技術、可靠度、尤其是安全性上的挑戰。本文以 VPLS、QinQ、Direct Connect 技術實際跨接 TWCC 及是方雲端交換中心雲平台和 AWS 的經驗，說明跨雲連接在技術上的挑戰及其解決之道。

關鍵詞：TWCC、CCX、跨雲環境、虛擬私有網路

Abstract

Along with the flourish of cloud computing, the coevolution of cloud service providers has led to the provision of similar services on the basis of divergent technology and advantages substantially specialized among different providers. In addition, due to the regulation constraints or security concerns, putting all kinds of data onto a single foreign cloud platform may not be desirable. Therefore, the combination of multiple clouds and on-premises facilities according to their individual advantages may lead to the best blend of functionality, cost effectiveness and security control. Based on our real experience, this paper introduces the challenges and our solution in building the inter-cloud environment among TWCC, CCX and AWS.

Keywords: TWCC, CCX, Inter-Cloud, VPN

1. 動機

自從雲端運算 (Cloud Computing) 異軍突起，成為計算環境的主流之後，如雨後春筍般大量崛起的雲端服務供應商 (Cloud Service Providers) 之間也產生了強烈的競爭，逐漸進入大者恆大、汰弱留強的發展成熟時期。2019 年市場上前三大的雲端服務供應商及其市佔率[1]分別為 Amazon AWS (32.3%) [2]、Microsoft Azure (18.1%) [3] 及 Google Cloud (6.2%) [4]。在激烈競爭下，各大雲端服務供應商所提供的基本服務項目雖然大致雷同，但各雲端服務供應商仍在技術、架構、定價、特殊服務等各方面演化出各自的特色及強項。此時視計算與服務的需求，便可能出現單一雲平台無法提供所有所需的功能、或是全部所需的功能均向同一雲平台獲取在定價上較為不利的情況。

以美國的 IceCube 微中子探測計畫為例。此計畫由美國加州大學聖地牙哥分校的 Igor Sfiligoi 及 Frank Würthwein 教授所領導的 EAGER 計畫團隊共同執行[5]，透過美國 Internet2 研網將 Amazon Web Services, Microsoft Azure, 及 Google Cloud Platform 三大雲端供應商的閒置 GPU 資源整合為單一計算資源池，並用以計算產自南極冰層下 1,450-2,450 公尺深的 5,160 顆光學感應器的高能粒子觀測資料。此計算共使用超過 51,000 顆 GPU，產生 380 PFLOP32 的計算力。此計算力比世界前三大超級電腦的計算力總合還多[6]。做為比較，我國所建置的台灣杉 2 號[7]在世界 Top 500 超級電腦排行榜中最新 2019/11 世界排名第 21 名，共有 2,016 顆 GPU，9 PFLOP 的計算力。很明顯地，上述 IceCube 探測計畫所需的計算資源必須跨雲整合方能獲得，並非單一雲端資源所能提供。

另一方面，受法規限制或商業機密考量，部份機敏性資料並不適合存放於境外的雲端空間或管控範圍外的計算設施上。然而自行建置全套硬體設施以滿足計算的需求，卻有事後管理維運人事成本高昂、資安管控不易、利用率低落、以及經濟規模小，採購不具價格優勢等缺點。相比之下，市佔率排名第一的 Amazon AWS 2019 全年投資金額超過台幣一兆元，位列第三的 Google Cloud 亦投資近台幣兩千億元[1]。且各大雲端服務供應商均有一流團隊進行設備維運及資安管控，個別的團體或公司在採購及建置規模上必定難以望其項背。此時若採用混合雲的模式，即將自有的計算設施與雲端資源進行整合，將機敏性資料保留

於自有設施處理，僅將不具機敏性的資料或是已濾去機敏資訊的計算工作分散至雲端處理，則可兼有兩者之長。

然而跨接多個雲端平台、或是跨接自有計算設施與雲端資源，除了會面臨資源控制整合上的挑戰之外，更會面臨跨雲連線的品質、可靠度及安全性的問題。在跨雲資源的整合及控管上，尚可部份仰賴各家業者所提出的異質雲端資源整合方案，例如最具開放性的 Google Anthos[8]，Microsoft 推出的 Azure Arc[9]，以及可跨公、私雲建立單一虛擬網路環境的 VMware NSX Datacenter[10]等。但此類方案所提供的 VPN 機制，最多僅能部份保障跨雲連線的安全性。由於一般跨雲連線需要穿越在各家雲端平台控制之外、且變動性極高的 Internet，因此上述方案對於跨雲連線的效能、可靠度及完整的安全性方面無能為力。然而跨接不同雲端平台的資源，首要便是居中的連線品質，否則立於其上的整體服務品質及可靠度俱為空談。透過骨幹網路及網路交換中心的服務，建立虛擬直連網路，以達成多雲之間的封閉式串接，將可同時滿足對於跨雲連線的保障頻寬、可靠度及完整安全性的要求。以下對於本文所跨接的 TWCC 及 CCX 雲、連線架構、所用技術分別加以介紹。

2. 相關技術介紹

2.1 TWCC

TWCC(Taiwan Computing Cloud，台灣 AI 雲)在國家前瞻基礎建設的支持下，由國研院國網中心銜命負責籌畫建置。主要提供雲端 AI 高速計算訓練服務、深度學習的容器化服務和推論分析的虛擬平台服務。TWCC 系統架構分為三個部分：(1)虛擬運算機器(VM)，底層採用雲端虛擬技術，可支援虛擬 CPU 和 GPU；(2)容器運算，以 Kubernetes 和 Docker 容器技術虛擬化 GPU 資源，提供專用且經優化過的深度學習框架的開發型容器和計算資源以排程共用方式的任務型容器；(3)高速運算服務(HPC)，透過開源軟體 Slurm 工具進行任務調度管理，且利用 Singularity 容器化技術做為大規模、跨節點的高速運算。TWCC 在 2019 建置初期是由 252 個節點所組成，具備 2,016 片 Nvidia Tesla V100 32GB GPU，效能達 9 PFLOPS。總儲存量達 10PB。TWCC 是國內第一套 AI 超級電腦，支援超過 300 餘專案計畫，橫跨國內產學研界各領域。

2.2 CCX 是方雲端交換中心

CCX(Chief Cloud eXchange，CCX)是方雲端交換中心[11]是由是方電訊所提供的連線服務，主要在多雲之間建立虛擬專用網路連線。CCX 與國際知名的雲服務供應商均有直接連線，可以打造具彈性的混合雲介接服務，有效降低企業租用國際連線費用，且可獲致最佳網路延遲和連線高可靠度。CCX 的骨幹網路是以 MPLS-VPN 技術建置，提供多點互連的虛擬私有網路，以流量工程(Traffic Engineering)保障網路服務的質量(QoS)。目前 CCX 與世界四大雲服務供應商直接建立私有網路連線：Amazon 雲平台的 AWS Direct Connect、Microsoft 雲平台的 Azure ExpressRoute、IBM 雲平台 Cloud Direct Link 和 Google GCP 雲平台的 Google Cloud Interconnect。TWCC 於 2020 年透過 QinQ Tunnel 技術與 CCX 建立直接連線，藉此虛擬專用通道與其他知名雲平台建立直通專線。

2.3 TWAREN

台灣高品質學術研究網路[12] (TWAREN，TaiWan Advanced Research and Education Network)是為學術研究而設的專用網路，服務對象包含國內各大專院校、政府機關及研究單位等。TWAREN 在架構設計上是一個高容錯備援性網路，提供 200 Gbps 的超高骨幹網路頻寬，支援網路第 1 層至第 7 層的各項連線及加值應用服務，也提供 20 Gbps 的國際連線頻寬，與美、歐、亞洲等地主要研網直接介接，並通過學術研究網路合作轉訊，與世界各國學術研究網路相連。

2.4 QinQ Tunnel

在區域網路的環境中，經常使用 IEEE802.1Q 虛擬網路(VLAN)的技術將大型網路區分為不同的網路群組，可以透過隔絕廣播封包網域來提升整體網路效能，虛擬網路是在網路封包的表頭上新增一個 4 bytes 的標籤，可以讓大型網路可依不同標記區分成最多 4096 個群組。近年隨著雲端網路與虛擬化的技術蓬勃發展，大型資料中心內虛擬網路標籤數量已不敷使用，為解決這樣的問題，QinQ VLAN 技術也因應而生。

QinQ VLAN 是 IEEE 802.1ad 標準，網路封包的表頭中帶著兩層虛擬網路(VLAN)標籤，除原來 IEEE802.1Q VLAN 的表頭 4bytes 標籤外，再增加一層 4bytes VLAN 標籤，視為兩層堆疊的封裝式 VPN 技術，簡單來說就是將使用者內層 VLAN 標籤封裝於骨幹網路的外層 VLAN 標籤當中，封包帶著兩層 VLAN 標籤穿越網路服務供應商的骨幹網路中，用戶的內層 VLAN 標籤可以自行分配不用擔心與骨幹網路的外層 VLAN 標籤衝突，不同用戶的內層 VLAN 標籤也能重複使用，只需在骨幹網路的外層 VLAN 標籤區隔唯一即可，使資料中心的網路可以有效率的管理，也大幅提昇雲端網路的擴充性。

3. 網路架構

3.1 AWS Direct Connect 連接

我們藉由 AWS Direct Connect 連接 AWS 和 TWCC 兩個公有雲。AWS Direct Connect 是專有通道，當我們需要在 TWCC 和 AWS 之間傳輸備份巨

量資料，或是因應組織企業應用需求，需要建立多雲平台的混合雲架構，使用該通道可以免去租用網際網路線路費，且避免大量封包流量占用網際網路連線，造成網路壅塞。除此之外，雲之間的傳輸更安全，以控制路由的方式，獲得網路延遲率達穩定的一致性；對於特定語音、視訊和高敏感度的應用可維持高可靠度。

在本論文圖 1 網路架構圖中，我們透過 CCX 建立 AWS Direct Connect，CCX 就近連結到位於東北亞區域 (ap-northeast-1) 日本東京的 AWS 閘道 DCGW(Direct Connect Gateway)，以 BGP 協定的私有自治系統編號(ASN)互相交換路由以建立連線。

在 AWS 下的虛擬網路稱為虛擬私有雲端 (Virtual Private Cloud，VPC)，一個 VPC 可以再切割數個子網路(subnet)，需要建立 Direct Connect 連線的子網路透過 VPC 的虛擬閘道(VGW)宣告出去；其他往 Internet 的訊務，往 IGW 閘道連外。在本例中是以 BGP ASN 64512 建立 VGW 和 DCGW 之間路由，並宣告 AWS 端的 VPC：10.22.22.0/24 網段進入 CCX，通過 CCX 的過境路由器(GW)，將路由再轉介到 TWCC。

TWCC 利用 TWAREN 骨幹與網際網路相連，位於 TWCC 出口的 TWAREN 邊際路由器(border router)與台北主節點和合作單位位於 CCX 機房的路由器建立端點到端點的 QinQ tunnel，透過該 tunnel 建立 TWCC 和 CCX 之間第二層虛擬私有網路的連接。TWCC 端的邊緣路由器(Edge Router)以 BGP AS65534 連接，宣告 TWCC 端的虛擬私有網段。

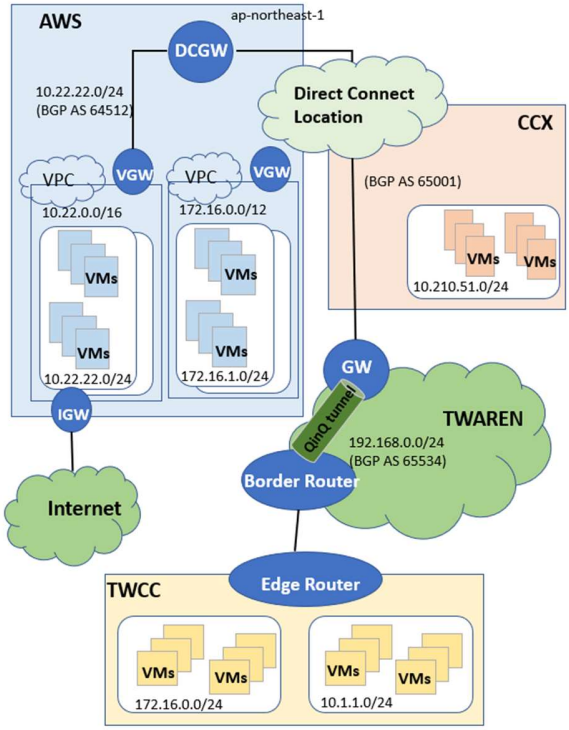

圖 1 網路架構圖

不同雲端平台本質上隸屬於各別的自治系統，執行各自的路由政策，跨雲整合不同雲端平台的計算資源，需要雙方各自分享彼此的路由資訊，而本論文提出的跨雲整合網路架構，是透過 TWAREN 骨幹網路及網路交換中心的服務，在 TWCC 與 CCX 雲端交換中心間建立虛擬直連連線，並透過 CCX 協助與各雲端平台交換、傳遞各自的 IP 路由，來達成網路互連的目的。BGP 使用 TCP 作為傳輸層協定，具備更可靠的路由更新，另外 BGP 的增量、觸發更新特性，只在有路由發生變動時才觸發路由更新，並且只更新變動的路由，穩定的路由並不會被送出更新，適合運作在不同自治系統間。為達到 TWCC 與各雲端平台之計算資源、儲存備份、服務監控等跨雲整合的目的，也考量後續整合各家雲端平台服務的擴充性，我們在 TWCC 與 CCX 之虛擬連線間建立多條 BGP 通道，並根據雙方路由政策宣告相應的 IP 路由，讓特定連線透過此虛擬直連網路直接互聯，避免走向連線品質、可靠度、安全性均難以控制的 Internet，藉以保障跨雲服務的連線品質。

3.2 BGP Peer 狀態及路由監控

為了提供高可靠度及高可用性的跨雲服務，並且快速、有效的偵測 TWCC 與 CCX 虛擬連線間底層的網路問題，我們針對路由器 BGP Peer 狀態、BGP Peer 路由內容進行監控，分別描述如下：

BGP 連線會經過六種狀態，分別是：Active、Connect、Open-sent、Open-confirm、Idle 和 Established，每個狀態代表 BGP 建立連線不同的過程，BGP Peer 狀態的最後一個狀態為 Established，達到此穩定狀態雙方即可開始宣告及交換路由。我們可以藉由監控 BGP Peer 狀態來判斷無法成功建立連線的原因，例如 BGP Peer 狀態卡在 Active，表示 TCP Handshake 無法建立，可能原因有 BGP Peer 不可達，或是 BGP 配置有錯誤。我們透過 SNMP 的方式來監控 TWCC 邊際路由器上的 BGP Peer 連線狀態，監控 TWCC 與各個雲端平台的 BGP Peer 狀態，也可實際反映跨雲服務的可用度，如圖 2 TWCC BGP Peer 狀態監控。

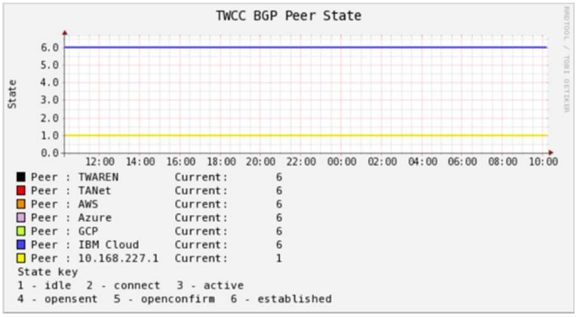

圖 2 TWCC BGP Peer 狀態監控

除了監控 BGP Peer 狀態之外，BGP 路由內容變化也會直接影響連線穩定性，在此我們監控各個雲端平台傳遞給 TWCC 邊際路由器的路由筆數，如圖 3，TWCC BGP 路由內容監控，路由缺

失或路由震盪會直接導致服務無法連通或連線不穩定，路由器頻繁地進行路由計算也會造成路由器負荷過重，若任一雲端平台因為錯誤配置造成路由內容變化導致服務無法連通，可以直接從監控圖表觀察出來。

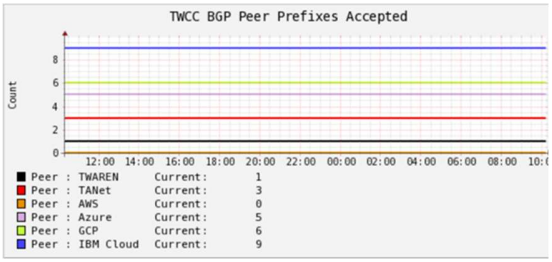

圖 3 TWCC BGP 路由內容監控

4. 挑戰及解決之道

4.1 QinQ tunnel

在 TWCC 與 CCX 跨雲平台第二層虛擬私有網路的互連上，由於中間並無直連電路，且國網中心並無專線接入 CCX，因此我們將跨雲平台互連切成兩塊，如圖 4 所示，由我方合作單位連線至 CCX 的第二層虛擬網路，TWAREN 利用骨幹的多點虛擬網路技術(VPLS)提供我方合作單位至 TWARN 台中主節點的連線。由於 TWCC 與 CCX 介接的混合雲連線可能依照不同需求會有多個不同的虛擬網路 VLAN 標籤需要通過骨幹網路，在技術上我們選用 QinQ VLAN 的方式，在骨幹網路中打通一條 VLAN Tunnel，讓兩個跨雲平台可依需求直接建立私有網路連線。

在骨幹網路 QinQ VLAN Tunnel 設定的過程中，我們發現合作單位使用的網路設備與國網中心使用的網路設備廠牌不同，QinQ VLAN 無法直接穿透整個骨幹，為了達成跨廠牌 QinQ VLAN 的透通，我們把 QinQ VLAN 的 Tunnel 也分成兩段，CCX 至我方合作單位獨立建立一個 QinQ VLAN Tunnel(如紅線所示)，合作單位至 TWAREN 台中主節點路由器獨立建立一個 QinQ VLAN Tunnel(如綠線所示)，兩個 Tunnel 在合作單位進行串接，最後達成跨廠牌 QinQ VLAN 的第二層虛擬私有網路通道。

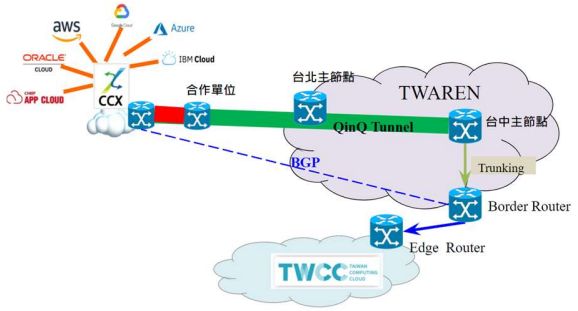

圖 4 QinQ tunnel 建置架構圖

4.2 MTU 所造成的問題

在 TWCC 與 CCX 順利連通之後，開始出現相當匪夷所思的 ssh 問題。雙方都可以通過 ssh 登入另一方環境所開設的虛擬機器，但隨後在執行 ls、top、cat 等指令時，經常會在執行結果顯示到一半時畫面及鍵盤失去回應。須要在使用者端手動 kill 掉 ssh 的 process，重新 ssh 連線才能排除。測試得到以下發現：

- 每次失去回應當掉的位置是一致的。
- 指令的顯示內容短時，就能正常執行。當顯示內容長時才會失去回應。
- cat 手動產生的特定長度檔案，發現會造成失去回應的檔案長度，落在 1450-1500 bytes 間。

測試結果暗示，當傳送內容一個封包可以傳完時即可正常執行；當封包需要切割時則會出現問題，因此極有可能為 MTU 的問題。進一步測試得到以下發現：

- TWCC VM 的 MTU 由 8550 改為 1500，問題依舊。
- 再進一步縮小為 1496，所有傳檔及指令就全部運作正常了。
- 此結果與從 ping -M do -s 1468 得到的結果相符。有效的 MTU 只有 1496，超過就有問題。
- 1496 和 CCX VM 端的 MTU 1500 只差 4 bytes。唯一這麼小的附加 header 只有 VLAN tag。
- 此結果暗示從 TWCC 到 CCX 的路徑上，有某一段的 MTU 只有 1500，但通過這一段的封包偏偏有貼 VLAN tag。

經調整加大 TWAREN 骨幹及連接 CCX 的 QinQ 線路的 MTU 後，MTU 1500 即可正確運作。顯示先前線路 MTU 設為 1500、然後被 VLAN tag 多限縮了 4 個 bytes，因而引起本次 MTU 問題的路段，是位在 TWAREN 骨幹或連接 CCX 的 QinQ 線路上。嘗試放大 CCX VM 的 MTU 但無法傳輸，顯示在 CCX 的 host 端或網路端 MTU 只有 1500。

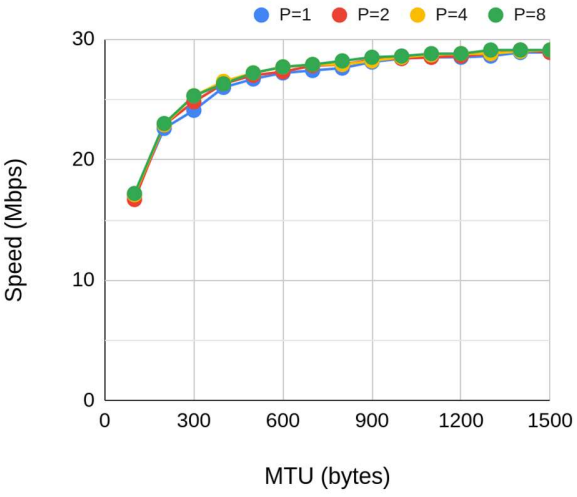

圖 5 TWCC 與 CCX 連線測速結果

使用 iperf3 對此段線路進行測速，雙向得到的結果均相同。不論使用 1、2、4、或 8 個 streams 同時進行傳輸，得到的結果均非常一致，隨 MTU 加大而飽和在 28.9 Mbps。此為 CCX 端 VM 的上端 supervisor VMware 使用了頻寬的限速功能進行軟體限速所致。如圖 5 所示。

4.3 路段 IP 重疊所產生的效應

在測試 TWCC 與 CCX 兩地的網路期間，觀察到了與其他計畫網路間的互通問題。檢視後發現在架構中隱藏了 IP 衝突的問題。

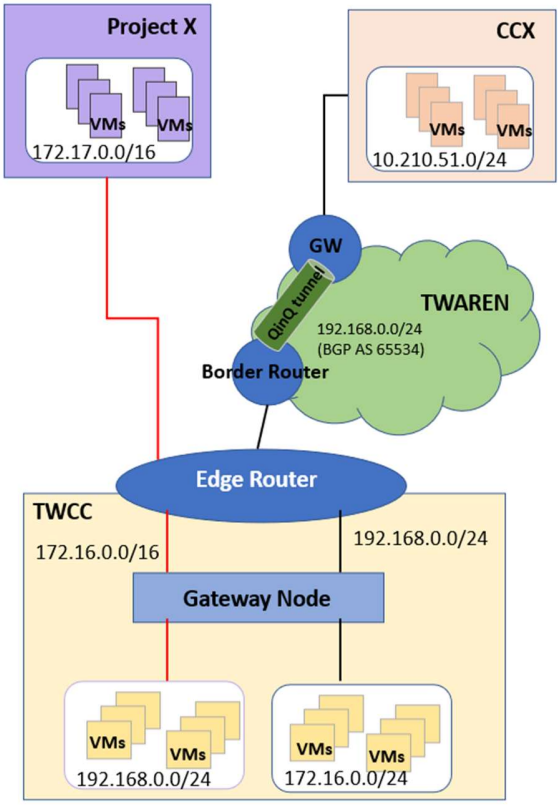

圖 6 TWCC 網路 IP 配置架構

TWCC 底層的基礎網路是採用 overlay network 架構，其中 overlay 技術是以 VXLAN(Virtual eXtensible LAN) id 做到邏輯切割，使得雲平台內的租戶虛擬網路彼此邏輯區隔，因此 VM 的虛擬網路可以自行設定網段。如圖 6，VM 的預設閘道是 Gateway Node，其扮演 DHCP 伺服器配發 IP 位址和 NAT(Network Address Translation)角色，將 VM 封包的來源 IP 轉換為浮動 IP(Floating IP)，該浮動 IP 可以為實體 IP，或是虛擬 IP，然後繼續向上送至邊際路由器進行後續的派送。因此從 IP 網段的觀點來看，TWCC 端共有 VM 至 Gateway Node 及 Gateway Node 至邊緣路由器兩段 IP 段。

在此次測試期間，意外觀察到與另一計畫間的網路互通問題。進一步分析後發現問題來自於兩個計畫所用的 IP 段有重覆。此兩個計畫事實上在任一個階層，IP 均未衝突，因此最初問題並未浮現。然而當兩個計畫間的網路需要互通時，送向對方網路的封包，卻會在 Gateway Node 與邊緣路由器之間遇上與目的地 IP 段相同的網段，造成封包抵達錯誤目的地 (與目的 IP 相同 IP 位址的網路設備) 或是目的 IP 無回應 (不存在) 而發生逾時錯誤。

事實上同樣的問題也存在於連接兩個雲端之間的線路中。以 CCX 及 TWCC 為例，從 CCX 對 TWCC 的 VM 進行 tracepath，可以得到以下的結果：

```
$ tracepath -n 192.168.0.4
 1?: [LOCALHOST]
 1:  10.210.51.254   0.422ms
 1:  10.210.51.254   0.555ms
 2:  113.21.84.249   0.370ms
 3:  172.30.53.6     3.515ms asymm  4
 4:  10.254.1.6      3.838ms asymm  5
 5:  10.42.217.45    7.920ms asymm  6
 6:  192.168.0.4     8.109ms asymm  7
```

由於專用網路的性質，因此兩端及途中經過的各段網路設備一般都是配置 private IP。造成有限的 private IP 資源被大量用在網路架構中。而 CCX 及 TWCC 均有相對複雜的架構以服務大量的客戶，因此 private IP 往往雙方皆已大量使用。要協商與雙方、及途經的網路都沒有衝突的 IP 段，難度即隨著架構的複雜而上升。同理可證，若要同時連接三方雲端資源、或交雜自有設施的混合雲，IP 的規劃便不可不慎，極易形成日後架構擴充、變動時未知問題的來源。

4.4 通過 CCX 使用 Amazon Direct Connect

使用一般雲端服務均須經由 Internet 接取。然而穿越 Internet 須通過不受使用者控制的網路區域，其路由、延遲時間、封包遺失率及壅塞程度等特性均無法事先得知，且會隨時間不斷變化。亦由於穿越不在掌控範圍內的 Internet，其傳輸安全性及 DNS 的可靠性亦易受駭客的負面影響。為了提供更可靠的服務品質，以 Amazon 為例，即提供 Direct Connect 服務。使用者直接連接至 Amazon 有進駐的網路交換中心，在實體網路與 Amazon 連接後，即可透過 Direct Connect 服務達成點對雲或雲對雲的直連。實際網路傳輸將由使用者連接交換中心的線路直接連至 Amazon 內部網路，全程走在已知的路徑上，且採用 private IP 進行連線，同時避免了 DNS 被劫持造成的資安風險。以 TWCC 與 Amazon AWS 位於美國西岸的資料中心所建立的 Direct Connect 為例，雲間通過的路徑如下所示。

```
$ tracepath -n 192.168.0.2
 1?: [LOCALHOST]
 1:  10.22.22.1              0.195ms     pmtu 1500
 1:  169.254.249.1           0.435ms
 2:  172.30.70.158           125.747ms asymm 13
 3:  172.30.70.157           125.682ms asymm 13
 4:  172.30.53.6             128.142ms asymm 13
```

```
5:  10.254.1.6          128.166ms asymm 13
6:  10.42.217.45        133.252ms asymm  5
7:  192.168.0.2         132.569ms
```

若兩個 VM 間改走 Internet，則從 TWCC 端至 Amazon 端的路徑為 TWCC → TWAREN → TWGate (洛杉磯) → Equinix 交換中心 (洛杉磯) → Amazon，而 Amazon 端至 TWCC 端則為 Amazon → TWGate (台灣) → TWAREN → TWCC。其中跨太平洋的部份，前往美國走的是 TWAREN 的國際線路，而返回台灣走的則是 Amazon 自有線路，來回不同路。來回延遲時間 (RTT) 則較 Direct Connect 長，達 170 ms 之久。使用 Direct Connect 的延遲時間與使用 Internet 不同，其原因為 Amazon 在台灣-美國西岸間具備自有線路，從美西的海纜上岸點至 Amazon 資料中心較為直接，相較之下 TWAREN 國際線路在上岸後需先連至位於洛杉磯的網路交換中心才連至 Amazon 資料中心，因此使用 Direct Connect 服務較通過 Internet 延遲時間較短。由於 Amazon 依建立 Direct Connect 服務時選擇的頻寬進行計費及限速，因此採用 Direct Connect 後的可得頻寬可能較使用 Internet 連接小。在本次研究中，通過 Direct Connect 的測速結果如圖 7。

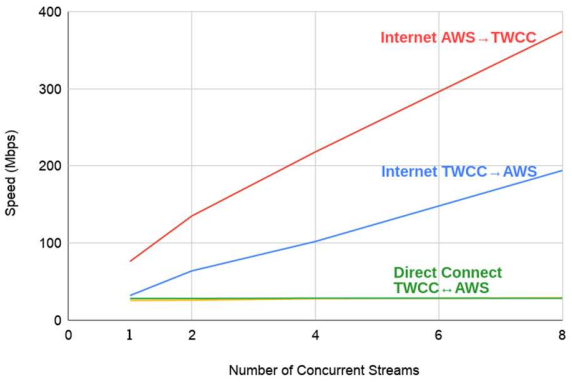

圖 7 採用 Direct Connect 及 Internet 的測速比較

使用 Direct Connect 進行兩個 VM 間的傳輸，雙向速率皆穩定飽和於 30 Mbps。此為本次研究所購買的頻寬，為限速的結果。而使用 Internet 進行傳輸時，沒有上述限頻的影響，兩個傳輸方向的傳輸速度均可隨同時傳輸的 stream 數量而等倍增加，可獲得遠高於 Direct Connect 的頻寬。且可觀察到流出 AWS 的方向可得速率較高的現象。

5. 結論和未來發展

對於高度重視安全性及服務整體可靠度的使用者而言，捨 Internet 而就專有線路，在交換中心與雲端服務供應商直連，是獲得訊務直接連接及最高傳輸可靠度的方法。對於條件不允許租用專線直接連接交換中心的使用者而言，透過骨幹網路所提供的 VPLS 服務以虛擬線路直連交換中心亦可達到同樣的目的。透過交換中心與雲端服務平台直連，可以確保訊務均只經過固定、已知且可靠的網路，避免中間人攻擊及 DNS 劫持的資安風險。對於整合兩個或多個雲端服務供應平台的資源、又或是將私有設施與雲端服務整合為混合雲來使用的使用者來說，使用交換中心直連或 Direct Connect 模式做為雲端連接的設計，將可確保跨雲的基礎設施擁有最高可靠度的基礎連線品質。

參考文獻

[1] Canalys, "Cloud market share Q4 2019 and full-year 2019 analysis report", https://www.canalys.com/static/press_release/2020/Canalys---Cloud-market-share-Q4-2019-and-full-year-2019.pdf, February 4, 2020.

[2] Amazon AWS, https://aws.amazon.com/tw/.

[3] Microsoft Azure, https://azure.microsoft.com/..

[4] Google Cloud, https://cloud.google.com/.

[5] Igor Sfiligoi and Frank Würthwein, "Running a 380PFLOP32s GPU burst for Multi-Messenger Astrophysics with IceCube across all available GPUs in the Cloud", NRP Engagement webinar, January 27, 2020.

[6] Top 500 Supercomputer List, https://www.top500.org/lists/2019/11/.

[7] 台灣杉 2 號 (TAIWANIA 2), https://www.twcc.ai/news/e80f2b49ea40515f74405e0a4e7fae197.

[8] Google Anthos, https://cloud.google.com/anthos/.

[9] Azure Arc, https://docs.microsoft.com/zh-tw/azure/azure-arc/.

[10] VMware NSX Datacenter, https://www.vmware.com/tw/solutions/multi-cloud-networking.html .

[11] CCX https://www.chief.com.tw/dispPageBox/ct.aspx?ddsPageID=CHDATASERVICE&dbid=4470337285

[12] TWAREN http://www.twaren.net/

[13] IEEE 802.1ad-2005: IEEE Standard for local and metropolitan area networks - Virtual Bridged Local Area Networks - Amendment 4: Provider Bridges.