

# 結合 5G Open RAN 與 TWAREN 的 MEC 建置

許維倫

國立中山大學 電機工程學系  
jackhsu007@atm.ee.nsysu.edu.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  
網路與資安組  
1203053@narlabs.org.tw

王博弘

國立中山大學 電機工程學系  
s94061910@atm.ee.nsysu.edu.tw

謝欣叡

財團法人國家實驗研究院  
國家高速網路與計算中心  
網路與資安組  
hsiehsr@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  
網路與資安組  
tlliu@narlabs.org.tw

許蒼嶺

國立中山大學 電機工程學系  
sheu@mail.ee.nsysu.edu.tw

李柏毅

財團法人國家實驗研究院  
國家高速網路與計算中心  
網路與資安組  
1203007@narlabs.org.tw

## 摘要

5GC (5G Core Network)通常使用集中式建置，不需要每一個學校都建置一套系統，目前許多研究型大學與國家高速網路與計算中心的 TWAREN 有連接，我們是第一個提出連結5G Open RAN 與 TWAREN 架構的論文，中山大學已經在校園建置一個5G Open RAN 實驗網路，我們可以透過校內網路對接 TWAREN，以及架設 MEC (Multi-access Edge Computing) Server 與其他 TWAREN 連結的大學採用 VPLS(Virtual Private LAN Service)多點連結，切出不同的 VLAN(Virtual LAN)確保不相互影響封包的傳輸，並進一步經由 Internet 連到雲端的 YouTube Server，本架構的特色是其它大學只要建置 RU (Radio Unit)、MEC Server，就可以透過 Internet 連上 YouTube Server，在此架構中，我們使用 MEC 攔截封包並做 Control Date 與 User Date 的分流，將 Control Date 回傳置5GC 進行註冊與認證，User Data 則直接傳至 YouTube Server，此架構可大幅降低封包延遲與封包遺失，並大幅度提升網路傳輸的 Data Rate。

關鍵詞：MEC, 5G Open RAN, VPN, 封包攔截與分流, TWAREN

## I. 前言

第三代合作夥伴(3rd Generation Partnership Project, 3GPP)[1]在第五代行動通訊技術定義 Open RAN 與 5GC 架構[2-3]，Open RAN 除了可以提供 Open Source 外[4-6]，還可以讓5G 專網建置者可以結合不同廠商設備來建置一套5G 行動通訊網路，例如:UE (User Equipment)、RU (Radio Unit)、CU (Control Unit)、DU (Distribution Unit)、5GC (5G Core Network)，5GC 是5G 行動通訊中的核心網路設備，其中的 UPF (User Plane Function)負責分流與轉傳，NSSF (Network Slice Selection Function) 負責提供選擇適當的網路切片，NRF (NF Repository Function)負責告知其他 NF (Network Function)的位置資訊，AMF (Access and Mobility Management Function)負責管理 UE 的連接、註冊、移動。VPN (virtual private network)為一種將專用網路 (例如校園網路) 延伸到公共

網路 (例如網際網路) 上的概念，透過 VPN 連線轉傳封包的優點包括增加專用網路的功能、安全性與管理，另外，5G MEC (Multi-access Edge Computing)是用來將封包攔截後再將 Control Data 跟 User Data 做封包分流，Control Data 往5GC 傳送完成註冊與認證程序，User Data 往目的地伺服器傳送。MEC 可實現控制與用戶平面分離 (CUPS, Control and User Plan Separation)，使用 CUPS 可以減少封包等待時間。舉例來說，假設使用者要看 YouTube，UE 在傳送封包時會發出一個訊號，透過 RU 連接光纖再傳到5GC，完成註冊與認證後，最後傳至 YouTube Server，這樣的傳送非常浪費網路資源並會增加使用者的等待時間，但是如果使用 MEC Server 並且整合 UPF (User Plane Function)的功能，封包傳到 RU 後可以進行攔截並執行封包的分流及轉傳，將註冊認證封包傳至 5GC 處理，User Data 直接傳至 YouTube Server，這樣的傳送可以減少網路資源的浪費，並減少使用者的等待時間。

本論文總共分為5個章節，除第一章為前言外，第二章介紹5G O-RAN 與 TWAREN，在第三章，我們提出一套機制來結合5G O-RAN 與 TWAREN，在第四章，我們設計控制與使用者封包分流的機制，第五章為結論。

## II. 5G O-RAN 與 TWAREN

### A. 5G O-RAN

5G NR (New Radio) 的 Layer 2，包含 PDCP (Packet Forwarding Control Protocol)、RLC 與 MAC 層[7]，根據 3GPP 定義其架構如圖 1所示。5G NR 協定分為兩個平面，分別為用戶平面(User Plane, UP) 及控制平面(Control Plane, CP)，兩者協定架構稍有不同。

用戶平面從上到下層依序為：

- SDAP 層：Service Data Adaptation Protocol
- PDCP 層：Packet Data Convergence Protocol
- RLC 層：Radio Link Control
- MAC 層：Medium Access Control
- PHY 層：Physical

控制平面從上到下層依序為：

- NAS 層：Non-Access Stratum
- RRC 層：Radio Resource Control
- PDCP 層：Packet Data Convergence Protocol
- RLC 層：Radio Link Control
- MAC 層：Medium Access Control
- PHY 層：Physical

從資料傳輸的觀點來看，從 Layer 1 進入 Layer 2 的 PDCP 層後，PDCP 自下層 RB (Radio Bearer) 取得資料後會將資料傳輸到 RLC 與 MAC 層，再從 MAC 層傳送到實體層(Physical Layer)。PDCP 層主要功能為，控制用戶平面傳輸、封包標頭(Header)的壓縮和解壓縮、資料加密和解密以及資料完整性的保護。PDCP 層將資料格式分為兩種，分別為標頭壓縮控制(Header Compression Control)與攜帶資料和序號(Sequence Number, SN) [7]。

RLC 層包含三種傳輸模式：

- Transparent Mode (TM)
- Unacknowledged Mode (UM)
- Acknowledged Mode (AM)

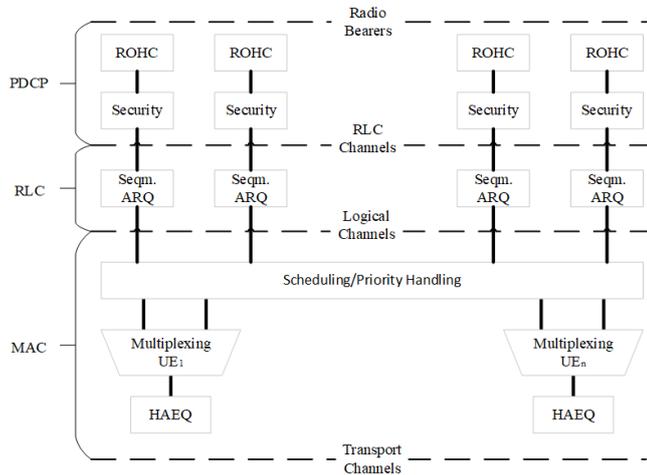


圖 1、5G NR Layer 2 Structure

#### A1. O-RAN

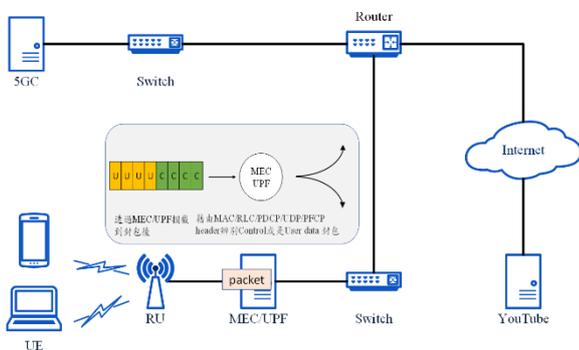


圖 2、5G O-RAN 架構

根據 3GPP 所定義的 5G O-RAN 架構[8]，如圖2所示，Open RAN 將傳統 RAN 分成三個單元，分別為無線電單元(Radio Unit, RU)、5GC 除了核心網路外還包含分佈單元(Distributed Unit, DU)、中央單元(Central Unit, CU)，RU 包含了天線與 Low-Physical (PHY)層，天線負責電磁波訊號的接收與傳送，Low-PHY 層負責波束成形 (beamforming)、快速傅立葉轉換(Fast Fourier Transform, FFT)、CP (Cyclic Prefix)的添加與去除等功能。DU 包含了 High-PHY 層、Media Access Control (MAC)層、Radio Link Control (RLC)層，High-PHY 層負責循環冗餘校驗 (Cyclic redundancy check, CRC)、打亂(Scrambling)、調變(Modulation)等功能，MAC 層負責排程(Scheduling)與多工(Multiplexing)等功能。CU 分為 CP 與 UP，CP 包含了 PDCP (Packet Data Convergence Protocol)的 CP 與 RRC (Radio Resource Control)，UP 包含了 PDCP 的 UP 與 SDAP (Service Data Adaptation Protocol)。

#### A2. 5GC

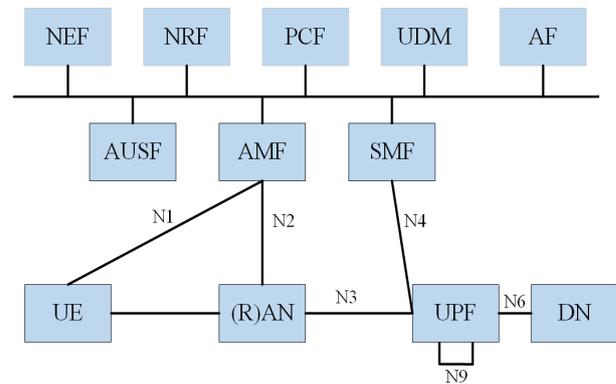


圖 3、5GC 架構

3GPP 定義 5G 核心網路 [2-3]，加入服務導向(Service-Oriented)的想法，因此 SBA (Service-Based Architecture)被提出，在 SBA 下，5G 核心網路拆解成許多獨立的網路功能(Network Function, NF)，其架構如圖 3所示。5GC 分成控制層與使用者層，控制層為 NSSF、NRF (NF Repository Function)、UDM (Unified Data Management)、AF (Application Function)、AMF、SMF (Session Management Function)、AUSF (Authentication Server Function)，使用者層為 UPF (User Plane Function)。NSSF 負責提供選擇適當網路切片的方法，NRF 負責告知其他 NF 的位置資訊，因此控制層的 NF 需要向 NRF 註冊，AMF 負責管理 UE 的连接、註冊、移動。

#### B. TWAREN

台灣高品質學術研究網路 (TWAREN, TaiWan Advanced Research and Education Network) [9]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 的特色包含: 100G 超高速骨幹網路、高容錯備援性網路架構設計、全面的國際研

網連線能力、多層次的網路服務，TWAREN 的技術包含全新的 VPLS VPN 服務，它是在網路架構的第二層上，如圖4所示[10-11]，TWAREN 有多點對多點的虛擬私有網路(Multipoint to Multipoint Layer 2 VPN)。它能在一個網路平台上提供多個虛擬私有網路，讓跨地區的校園或辦公室網路連結模擬成在同一區域網路，它使用共同資源時會更加便利。此服務平台亦針對跨地區的合作計畫或測試提供具有彈性的 VPN 網路服務。

VPLS 的使用有下列4種情境：

- 校本部與分校的校園網路連接
- 組織本部與分部的網路連接
- 醫院與醫院連結
- 建構測試網路平台

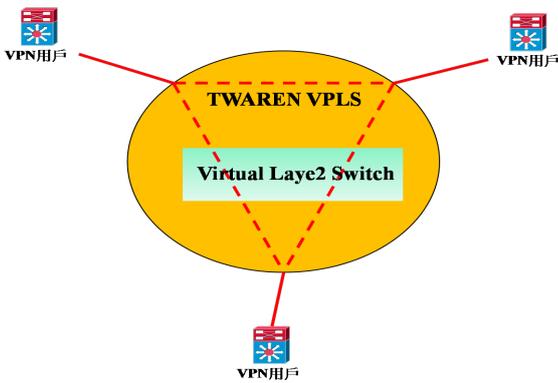


圖 4、VPLS 服務連線架構之邏輯示意

中山大學是 TWAREN 的連接點之一，我們設計兩種方案，如圖5所示，它可以讓中山大學的無線寬頻研究中心連接至 TWAREN。

- AB 間連線：由光纖連至中山大學海工館。
- BC 間連線：
  - 第一種方式：在校內重新拉一條光纖，但成本比較高。
  - 第二種方式：利用校園間原有的線路，並切出一個專用的 VLAN ID。如圖 5 中的紅線。
- CD 間連線：
  - BC 間連線如使用第一種方式，這段就不用接，可直接從光纖 Panel(C) 到校內網路的 Router 或 Switch(D)再拉另外一條線路。
  - BC 間連線如使用第二種方式，則用原本的線路。
- DE 間連線：
  - BC 間連線如果是使用第一種方式，就是從光纖 Panel (C) 到 E，線材採用 ST-LC。
  - BC 間連線如果是使用第二種方式，就是從 D 設備拉線到 E，線材採用 LC-LC。

### III. 結合 5G O-RAN 與 TWAREN

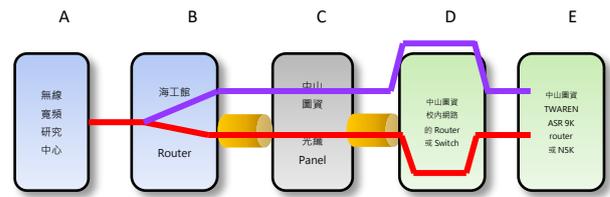


圖 5、中山大學與 TWAREN 連接架構

#### A. Wireless UE 到 Cloud Server

如圖6所示，當使用者(UE)上傳一部影片到 YouTube 時，UE 會先傳送認證、註冊封包，然後接著傳送 Video 封包，當 RU 將封包傳到 MEC/UPF Server 時，MEC/UPF Server 會將認證與註冊封包傳至中山大學的 5GC 處理，而 Video 封包則直接傳至 YouTube Server。

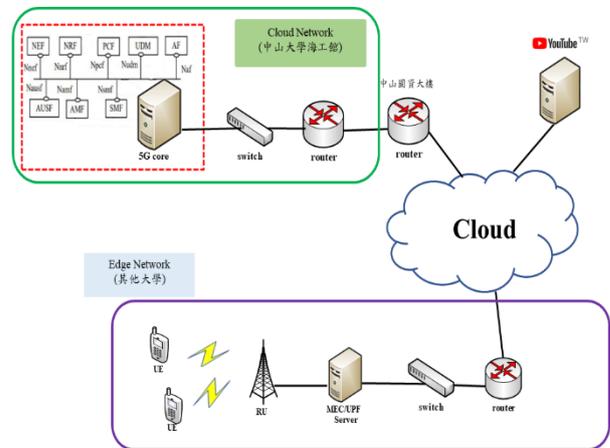


圖 6、UE 到 Cloud Server 的 MEC 架構

#### B. VPN/NAT 轉址

VPN (Virtual Private Network) 為一種將專用網路 (例如校園網路) 延伸到公共網路 (例如網際網路) 上的概念，讓使用者能夠共享或公共網路上傳送和接收封包，就好比我們的 UE (User Equipment) 直接連接到了專用網路上；透過 VPN 連線轉傳封包的優點包括增加專用網路的功能、安全與管理，此外 VPN 亦提供對網際網路上無法存取的資源進行存取，對於 VPN 協議的技術而言專家們也提出了許多不同的方法來進行，較常見的為點對點隧道協定 [12-15]：

點對點隧道協定 (Point to Point Tunneling Protocol, PPTP)：是由 Microsoft 與 3Com 等公司組成的 PPTP 論壇開發的一種 Point-to-Point Tunneling Protocol。PPTP 的運作方式是藉由將網路協定資料段封裝 (Encapsulated) IP Packet 透過 Router 來傳送，經過包裝之後的 Packet 會被網路上的 Router 視為一般的 IP Packet，直到抵達通道的另一端之後，才將傳送端所添加上去的 IP Header 移除。此種 IP Tunneling 封裝的好處是可以讓許多不同協定的資料能夠經由僅支援 IP 的網路媒介傳送。

C. MEC/UPF 分流

如圖2所示，當使用者透過 UE 傳送資料時，UE 發送訊號到基地台後，透過 MEC/UPF (User Plane Function) 做封包攔截，MEC/UPF 會藉由封包的由 MAC/RLC/PDCP/UDP/PFCP (Packet Forwarding Control Protocol) header 中先辨別是 Control Data 還是 User Data，經過此辨識後就可以做封包分流。

IV. 控制與使用者封包分流

A. 5G-MEC 層級架構

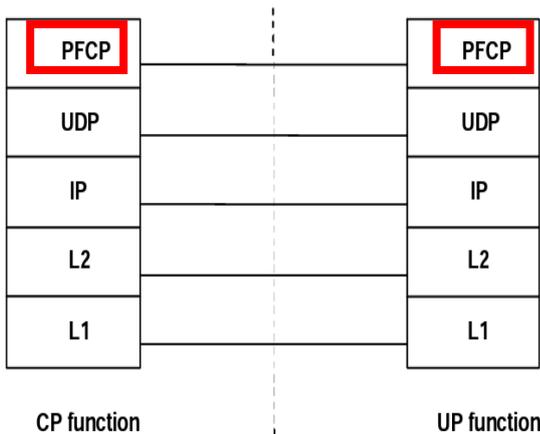


圖 7、5G PFCP

如圖7所示，根據3GPP TS 29.244所制定[7]，數據封包轉發控制協議 (PFCP) 是透過 N4 接口 (如圖3所示) 進行控制平面和用戶平面功能之間傳送。PFCP 是5GC 中引入的主要協議之一，PFCP 也使用於4G/LTE EPC 中以實現控制和用戶平面的分離 (CUPS)。PFCP 和相關接口主要將移動核心網絡中使用不同類型功能元素之間的交互形式化，大多數運營商都部署了這些功能元素，為移動用戶提供4G和5G服務[16-17]。為下列這兩種類型組件：

1. 控制平面 (CP) 功能元素: 主要處理信號過程 (例如網絡連接過程、用戶數據平面路徑的管理，還有一些輕量級服務作為 SMS 的交付)。
2. 用戶數據平面 (UP) 功能元素: 主要處理數據封包轉發，基於 CP 元素設置的規則 (例如 O-RAN 上)。

PFCP 封包格式如圖8所示，一個 PFCP 封包的 Message Format 中有 Message Type，Message Type 的對應功能如圖10所示，不同的 Message Type 有不同的功能，例如: Message Type 中的 Request=1，Response=2，就是代表建立一條 CP 與 UP 的連線。

如圖9所示，PFCP Information Element Format 中有 IE length，IE length 被定義為具有專門編碼或分組編碼。分組編碼的 IE length 只是其他 IE length 的列表，是一個接著一個的編碼。IE length 類型從 0~32767，是3GPP 所優先使用的，IE length 類型從 32768~65535 可以自己

定義使用，但是企業 ID 必須設置為發行方的 IANA SMI 網絡管理私有企業代碼。

圖10為 PFCP Message Format 的 Standardized Message Types，它是用來規劃不同的 Request 與 Response，例如: 當 Request=50，Response=51時，可從 CP (Control

Bit/Byte offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Bytes 0..3	Version (1) (spare bits)				MP / S				Message Type								Message Length (in bytes, not including the first 4)															
Bytes 4..11	if (S flag set) then SEID; else these bytes are missing																Sequence Number		if (MP flag set) then Message Priority; else (spare bits)				(spare bits)									
Bytes 8..11																																
Bytes 4..7 or 12..15																																
Bytes 8..(MsgLen-4) or 16..(MsgLen-4)	Zero or more Information Elements																															

圖 8、PFCP Message Format

Bit/Byte offset	1~15	16~31
Bytes 0..3	Type	IE Length (in bytes, not including the first 4)
Bytes 4..IELen+4	if (Type >= 32768) then Enterprise-ID; else this is part of the Payload	Payload (cont.) ...
	Payload cont. ...	

圖 9、PFCP Information Element Format

Message Type	Req	Resp	Message	Interface Applicability				Direction		Purpose
				Sxa	Sxb	Sxc	N4	Req	Resp	
0			(Reserved)							
(1..49)	Node Related Messages									
1	2		Heartbeat	X	X	X	X	CP ↔ UP	Can be optionally used between communication peers which have an established association, to check if the other node is alive. A Recovery-Timestamp is used to detect if the other peer has been restarted.	
3	4		PFD Management	-	X	X	X	CP → UP UP → CP	Optional feature, to provision PFDs per Application identifier, outside of the regular PFCP sessions.	
5	6		Association Setup	X	X	X	X	CP ↔ UP	Setup and update an association between CP and UP functional elements. Includes list of optional features, to inform the other elements about capabilities; other configuration elements are passed as well. No session related messages should be exchanged before this procedure.	
7	8		Association Update	X	X	X	X	CP ↔ UP	While the Association-Release is only triggered by the CP, the UP can request it as part of the Association-Update-Request.	
9	10		Association Release	X	X	X	X	CP → UP UP → CP		
-	11		Version Not Supported	X	X	X	X	CP → UP UP → CP	Error response to all requests which do not cover the implemented versions (currently only version 1 defined).	
12	13		Node Report	X	X	X	X	UP → CP CP → UP	Sent by the UP function to report information which is not part of a session, but potentially general (e.g. user-plane path failure).	
14	15		Session Set Deletion	X	X	-	-	CP → UP UP → CP	Sent by the CP function to indicate a partial failure, requesting deletion of all sessions affected.	
(50..99)	Session Related Messages									
50	51		Session Establishment	X	X	X	X	CP → UP UP → CP	Used by the CP to setup, modify and remove sessions consisting of sets of rules for processing and forwarding UP traffic. These are the main functional message of the PFCP application domain.	

圖 10、Standardized Message Types

Plane)來設置、修改和刪除由 UP (User Plane)處理和轉發的封包。

### B. 封包攔截與轉向

如圖11所示，Control Data 會沿著圖中綠色箭頭方向，經過 switch、Router、Switch 再到 5GC 去做註冊認證。User Data 會沿著圖中橘色箭頭方向，經過 Switch、Router、Internet 最後傳送到 YouTube Server 做儲存。

我們設計並實作三種結合 5G Open RAN 與 TWAREN 的 MEC 建置機制，第一種機制為使用者要上傳影片至 YouTube，第二種機制為使用者要從 YouTube 下載影片觀看，第三種機制為其他大學要透過 TWAREN 連至中山大學使用 5GC 進行註冊與認證。

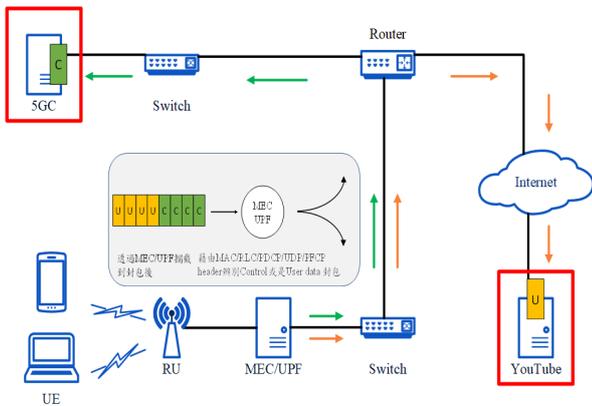


圖 11、Control and User Data 封包分流

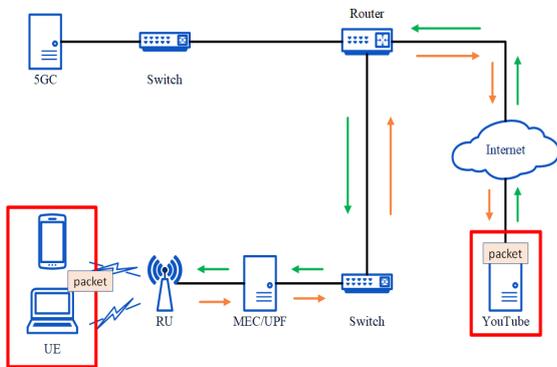


圖 12、使用者透過 YouTube 上傳下載影片

如圖12所示，當使用者要上傳影片時會沿著圖中橘色箭頭方向，透過 UE、基地台、MEC/UPF Server、Switch、Router、Internet 再傳到 YouTube Server，這樣可以減少封包要先到 5GC 註冊認證後再回到 YouTube Server 的時間。當使用者要下載影片時會沿著圖中綠色箭頭方向，會直接透過 YouTube Server、Internet、Router、Switch、MEC/UPF Server、基地台再傳至 UE，一樣可以減少訊號要先到 5GC 再回到 UE 的等待時間。

如圖 13 所示，其他大學透過 TWAREN 使用 5GC 上傳影片到 YouTube 時，UE 傳送註冊、認證、Video 封包到 RU，這些封包會透過各大學自己的 MEC/UPF Server 進行分流，註冊與認證的封包會沿著圖中綠色箭頭方向，經由 TWAREN 到台南國網中心後，再透過 TWAREN 傳回中山大學的 5GC 進行處理，但是 Video 封包不用傳到中山大學的 5GC，會沿著圖中橘色箭頭方向直接經由 Internet 傳到 YouTube Server。

如圖14所示，其他大學透過 TWAREN 使用 5GC 下載 YouTube 影片觀看時，同樣的，UE 傳送註冊、認證、Video 封包到 RU，這些封包會透過各大學自己的 MEC/UPF Server 進行分流，註冊與認證的封包會沿著圖中藍色箭頭方向，經由 TWAREN 到台南國網中心，再透過 TWAREN 傳回中山大學的 5GC 進行處理，但是 YouTube 的 Video 封包不用傳到中山大學的 5GC，Video 封包的傳送路線如圖中紅色箭頭所示，從 YouTube Server 先經由 Internet 傳到各大學 MEC/UPF Server 後，再經由 RU 傳到 UE 端進行播放觀看。

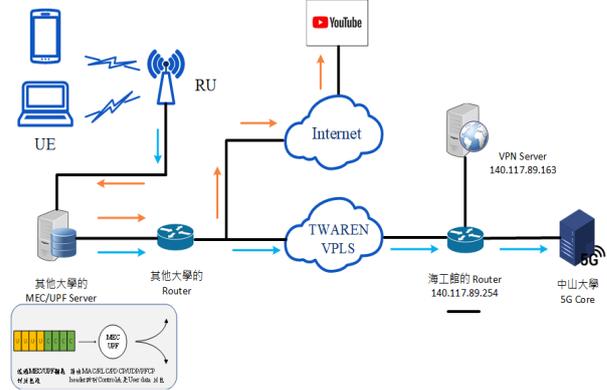


圖 13、其他大學透過 TWAREN 使用 5GC 上傳影片到 YouTube

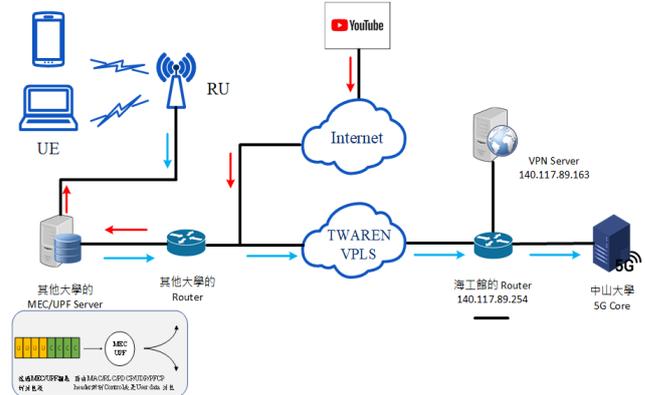


圖 14、其他大學透過 TWAREN 使用 5GC 下載 YouTube 影片

## V. 結論

本論文提出一個結合5G Open RAN 與 TWAREN 的 MEC 建置機制，我們已經實作完成5G Open RAN 與 TWAREN 連接，並完成架設 MEC Server，其他大學也可透過他們的 MEC Server 連接 TWAREN，到中山大學進行註冊認證，並進一步經由 Internet 連到 YouTube Server。本論文的特色是其它大學只要建置 RU 與 MEC Server 就可以透過 Internet 連上 YouTube Server，在此架構中，我們使用 MEC Server 攔截封包並做 Control Date 與 User Date 的分流，Control Date 先回傳置中山大學的 5GC 進行註冊與認證，User Data 則可以直接傳至 YouTube Server，此架構可大幅降低封包延遲與封包遺失，並大幅度提升網路傳輸的 Data Rate。另外，本論文也實作完成三種結合 5G Open RAN 與 TWAREN 的 MEC 建置機制，第一種機制為使用者要上傳影片至 YouTube，第二種機制為使用者要從 YouTube 下載影片觀看，第三種機制為其他大學要透過 TWAREN 連至中山大學透過 5GC 進行註冊與認證，當註冊認證完成後，使用者就可以直接到 YouTube Server 上傳或下載影片。

## 參考文獻

- [1] 5G: Study on New Radio(NR) Access Technology,"3GPP TR 38.912,Ver.15.0.0,Release 15 ,Sep.2018.
- [2] Li, J., Cao, X., Guo, S., Dong, R., Song, C., Wang, T., & Wang, Z. (2021, December). 5GC Network and MEC UPF Data Collection Scheme Research. In 2021 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM) (pp. 80-85). IEEE.
- [3] Lin, L., Zhu, B., Wang, Q., Xu, L., & Mu, J. (2020, December). A novel 5g core network capability exposure method for telecom operator. In 2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCLOUD/SocialCom/SustainCom) (pp. 1450-1454). IEEE.
- [4] M.A Habibi, M.Nasimi,B.Han, and H.D.Schotten, "A comprehensive Survey of RAN Architect Toward 5G Mobile Communication System," IEEE Access Vol. 7,pp.70371-70421,May 28,2019.
- [5] Singh, S. K., Singh, R., & Kumbhani, B. (2020, April). The evolution of radio access network towards open-RAN: Challenges and opportunities. In 2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW) (pp. 1-6). IEEE.
- [6] Chih-Lin, L., Kuklinski, S., & Chen, T. (2020). A Perspective of O-RAN Integration with MEC, SON, and Network Slicing in the 5G Era. IEEE Network, 34(6), 3-4.
- [7] 3GPP," 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; NR; NR and NG-RAN Overall Description", 2th Release 15. Lisbon, 2017
- [8] 劉則毅, "在5G-SA-Open RAN 的動態調整影音串流機制", 中山大學碩士論文。
- [9] 楊哲男, 古立其, & 劉德隆. (2019). The Implementation of High Performance Data Transfer over TWAREN International Connectivity. TANET2019 臺灣網際網路研討會, 488-492.
- [10] 呂宗翰, & 楊哲男. (2018). SSL-VPN 服務建置於 TWAREN VPLS 網路. TANET2018 臺灣網際網路研討會, 420-424. 虛擬私有網路 (Virtual Private Network, VPN) . 2012.
- [11] 周大源, 楊哲男, 古立其, & 劉德隆. (2019). 視覺化 TWAREN 高速資料傳輸網路系統之效能優化機制實作. TANET2019 臺灣網際網路研討會, 498-503.
- [12] 虛擬私有網路 (Virtual Private Network, VPN) . 2012; from: <http://webftp.cogsh.tp.edu.tw/cti573/bcc2012/handout/vpn.htm>
- [13] Zhao, J., Ni, S., Yang, L., Zhang, Z., Gong, Y., & You, X. (2019). Multiband cooperation for 5G HetNets: A promising network paradigm. IEEE Vehicular Technology Magazine, 14(4), 85-93.
- [14] Ezra, P. J., Misra, S., Agrawal, A., Oluranti, J., Maskeliunas, R., & Damasevicius, R. (2022). Secured communication using virtual private network (VPN). Cyber Security and Digital Forensics, 309-319.
- [15] Tongkaw, S., & Tongkaw, A. (2018, November). Multi-VLAN Design over IPsec VPN for Campus Network. In 2018 IEEE Conference on Wireless Sensors (ICWiSe) (pp. 66-71). IEEE.
- [16] Zhao, J., Ni, S., Yang, L., Zhang, Z., Gong, Y., & You, X. (2019). Multiband cooperation for 5G HetNets: A promising network paradigm. IEEE Vehicular Technology Magazine, 14(4), 85-93.
- [17] do Amaral, T. A. N., Rosa, R. V., Moura, D. F. C., & Rothenberg, C. E. (2021, October). An In-Kernel Solution Based on XDP for 5G UPF: Design, Prototype and Performance Evaluation. In 2021 17th International Conference on Network and Service Management (CNSM) (pp. 146-152). IEEE.