

桃園區域網路中心

「臺灣學術網路(TANet)區域網路中心 114 年度
基礎維運與資安人員計畫」

計畫期程：114.1.1~114.12.31

計畫執行單位：國立中央大學

國立中央大學電子計算機中心
中華民國 113 年 12 月

1 計畫基本項目

1.1 計畫期程

本計畫為 TANet 桃園區域網路中心基礎維護與管理運作及資安人員、北區教育雲計畫。計畫期程：民國 114 年 1 月 1 日至民國 114 年 12 月 31 日止，為期一年。

1.2 計畫執行單位

本計畫執行單位為：國立中央大學。國立中央大學自 TANet 臺灣學術網路創建至今日，一直積極參與 TANet 臺灣學術網路的發展，擔負桃園區網中心維運重任，桃園區網中心目前提供桃園、金門、連江地區三百多所各級學校介接全球 Internet 網際網路，包括：桃園市、金門縣及連江縣三個國中小教育網路中心，及多所大專院校、學研單位及高中職等學校。

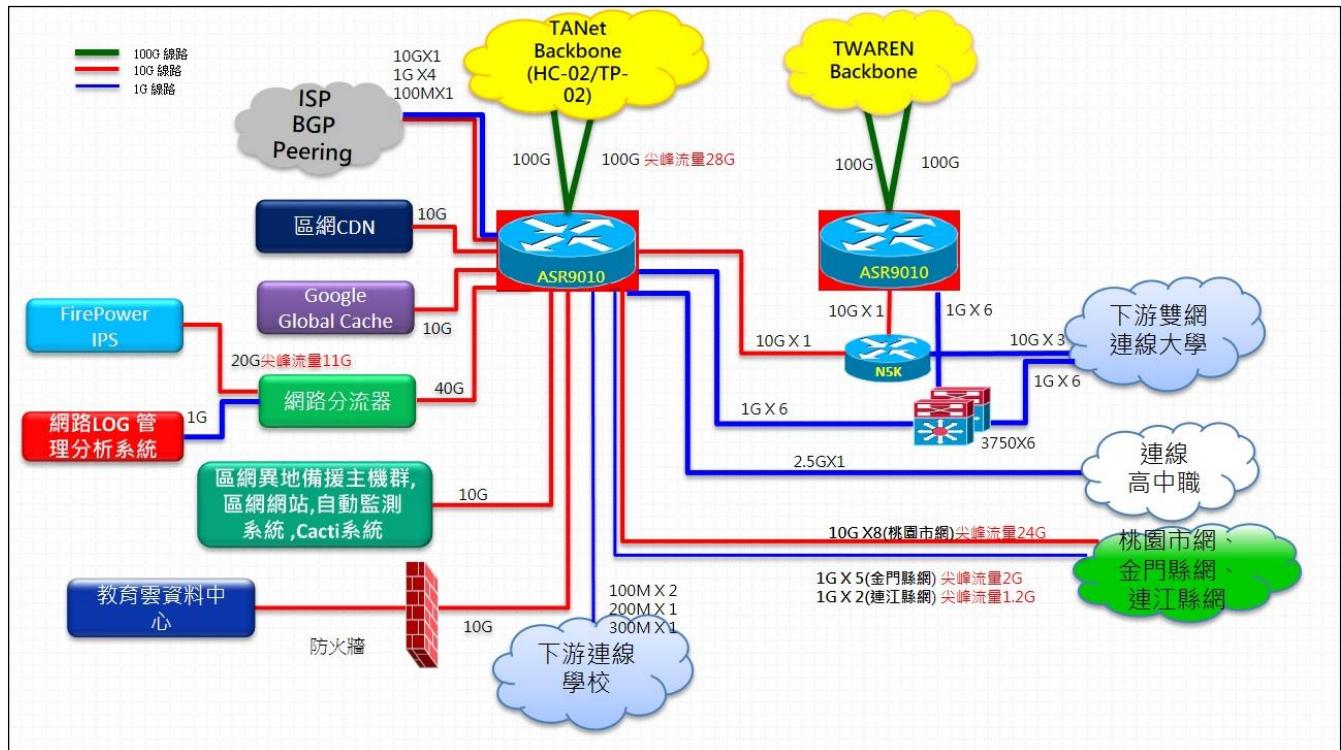
2 區域網路中心基本維運

2.1 現況說明(含網路架構圖)

2.1.1 目前工作、任務及網路連線情形

桃園區網骨幹 Router 以 100 Gbps 頻寬連接至 TANet 骨幹網路，並分別與國內多家網路 ISP 業者（如中華電信 Hinet、Seednet、台灣固網、亞太線上 APOL 等）分別以 10 Gbps、1Gbps 專線作多點互連，快速交換網路資訊。如圖 1 所示。

圖 1. 桃園區域網路架構圖



區網中心除提供桃園地區大專院校、學術研究單位及高中職等共 38 個單位之連線界接 TANet 外、也接有桃園市、金門縣及連江縣等三個國中小教育網路中心，目前共計有桃園區域的三百多所各級學校透過桃園區網中心介接全球 Internet 網路。

為加強與各連線單位管理經驗之交流，區網中心每年召開至少兩場的區網管理與技術小組會議、舉辦多場的網路技術、資訊安全研討會，並建置區網中心網站，連線學校伺服主機檢查系統，桃園區網 LINE 群組等溝通介面，提供方便有效的資訊交換平台。

2.1.2 電力與空調建設

為能維持桃園區網機房的良好運作，提供更高品質的連線品質，桃園區網中心已陸續增設大容量的發電機組，包含 450KVA 發電機組及配電線路及 500KVA 發電機組 1 座，並具備切換二部發電機之開關；二座模組式 UPS(200K-A, 200K-B)，以及三台 10 噸冷氣與 1 台窗型冷氣等空調系統，無須再擔憂台灣電力公司及區網節點學校的年度維護工作，與其他無預警等停電事故對區網機房運作的影響。另外為加強機房環境監控也建置網路機房溫度計、溫度監看網頁，以及攝影系統及機房門禁刷卡系統。

2.1.3 連線單位之組織與協調

為增進連線單位管理經驗之交流，區網中心除了每年定期召開區網管理與技術委員會會議、提供網路連線、網路安全與管理相關諮詢外，也定期辦理多場的主題式研討會及重點式技術研習。例如：防範駭客及病毒、資安技術教育訓練、不當資訊防治、智慧財產權宣導。並已著手協助連線學校進行網站弱點掃描、連網主機健檢等資安服務的活動。

以 113 年為例，桃園區網第 73 次管理會議於 4 月 26 日在體育大學舉辦，連線單位出席率 92% (現場人數+線上人數)，議程進行區網業務報告、資安通報與應變及資安宣導，第五屆傑出網管人員頒獎。邀請南亞技術學院資訊圖書中心黃琮淵主任「智慧校園 homeassistant 應用」、清華高中呂聖傑老師「穩定的校園網路規劃及資料保護」經驗分享。第 74 次管理會議於 10 月 17 日在臺北商業大學桃園校區舉辦，連線單位出席率 94% (現場人數+線上人數)，議程進行區網業務報告及資安宣導，第六屆傑出網管人員選拔，邀請開南大學蔡孟修技佐「工作經驗分享」、萬能科大陳信呈組長「網管的日常」二位連線學校老師經驗分享，並特別邀請張家倫老師、謝勝任老師演講 eduroam 導入與無線漫遊向上集中。

桃園區網中心建有桃園區網網站 (<https://www.tyrc.edu.tw>)，以使用者為中心提供更友善服務，首頁即可顯示主要網路目前使用率，並加入建立網管、資安技術問題集 FAQ，供連線學校查詢，可提供連線學校老師先自行排除問題，並節省區網人員回覆問題的工作量。

此外，區網中心也開發桃園區網網管通訊錄，協助連線學校掌握網路服務狀況，也建立桃園區網 LINE 群組作為即時的溝通交流與快速的狀況處理，分享網管工具、網路服務與管理經驗。

- 桃園區網中心網站 <https://www.tyrc.edu.tw>
- 桃園區網網管通訊錄 <https://portal.tyrc.edu.tw/> (須用帳號登入)

2.1.4 教育推廣活動之規劃

因應網路駭客、網頁資料竄改、勒索病毒、網路詐騙等資安事件，網管人員無法僅僅依賴技術上的防制措施解決問題，還必須多利用教育訓練來宣導正確觀念的建立，對抗層出不窮的網路問題。

因此，區網中心每年均舉辦多場的網路技術、資訊安全研討會，並將課程教材上網，提供如：資安實作 Workshop、資安及個資保護、智慧財產權宣導、防範駭客及病毒、網路安全、雲端系統、網路管理工具及網路系統的建置。

2.1.5 網路服務系統及設備

桃園區網中心建置及管理的網路服務系統均提供一年 365 天 24 小時不間斷的運作以供本地區連線單位使用。區網中心提供的服務系統包括：骨幹連網 Router、Domain Name Server、區網中心 WWW、異常流量偵測、Top-N 訊務排行、IP 管理資訊查詢網站、連線單位流量監看 MRTG 網站、IPv6 監控/mrtg 等多項服務、異地備份、異地備援服務（詳見表 1）。

表 1 TANet 桃園區網主要服務系統

| | | |
|----|---|--|
| 1 | 骨幹連網 Routers: ● 提供區網界接 TANet 100G 骨幹網路 ● 提供 ISP 區域互連網路 ● 提供桃園區域學校以光纖連線區網機房 | Cisco ASR9010 Router |
| 2 | Domain Name Server (DNS) ● Domain: tyrc.edu.tw tyc.edu.tw | Master server: ● dns. tyrc. edu. tw (140.115.2.1) ● Slave name server (140.115.1.33) ● webdns. tyc. edu. tw (163.30.4.201) ● Slave name server: (192.192.227.4) (140.115.1.33) |
| 3 | 區網中心 WWW 網站提供各項資訊包含： ● 網路管理、資訊安全、教育訓練等訊息公告。 ● 網路流量 ● 資安服務 ● 區網中心歷年度工作報告、會議記錄 ● 常見網管、資安問題 FAQ | https://www.tyrc.edu.tw |
| 4 | 網管通訊錄 | ● https://portal.tyrc.edu.tw/ (須用帳號密碼登入) |
| 5 | IP 管理資訊查詢服務，提供：連線學校 IP 查詢 | ● https://www.tyrc.edu.tw/IPv4 |
| 6 | 連線單位流量 Cacti 監看 ● 提供連線學校監看的連線狀況與及時流量圖 | ● https://cacti.tyrc.edu.tw/tyrc.html |
| 7 | Zabbix 自動監測系統 ● 針對重要網路設備、實體及虛擬伺服器的服務效能監測。 | ● https://zabbix.tyc.edu.tw |
| 8 | 資安檢測及弱點掃描 ● 提供桃園區網連線單位申請弱點掃描(IP)及網頁檢測(Web)檢測。 ● 使用 APP Scan 及 Nessus Pro 做為檢測工具 | ● https://www.tyrc.edu.tw/security |
| 9 | 資安維運中心(SOC)建置 ● 入侵偵測/攔阻 IDP 設備 ● 入侵事件通告/回報系統 | ● CISCO FirePower Security Platform |
| 10 | 異地備份、異地備援主機 | ● Synology NAS，僅對申請連線單位開放 |

2.2 工作內容

隨著網際網路的快速成長，TANet 也陸續呈現：網路濫用導致壅塞、不適資訊之流竄、病毒

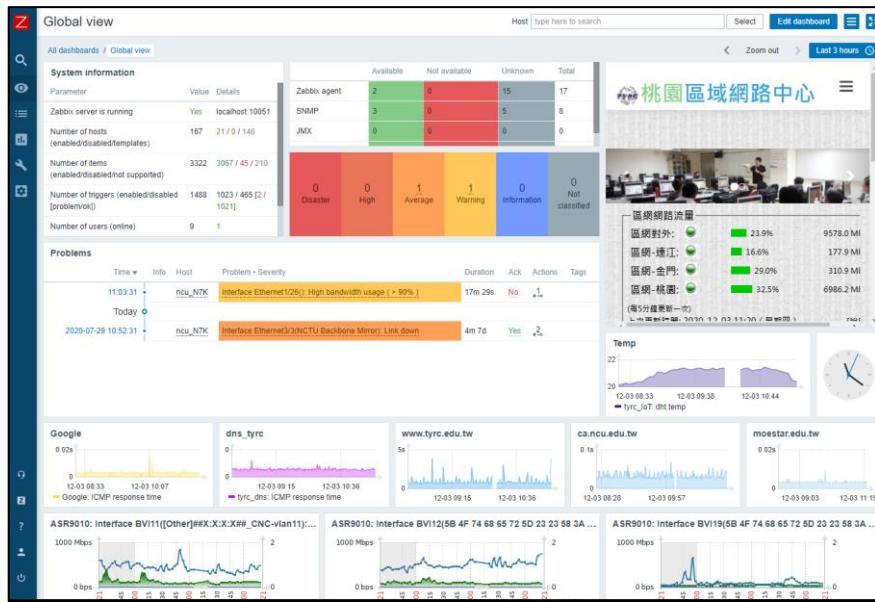
肆虐、駭客入侵等問題。由於區網及縣市網中心分擔了 TANet 的管理及運作，能否積極並有效率地和骨幹及連線單位保持互動及協調合作，是每一區網或縣市網中心能否順暢運作的重要因素。為解決這些問題，本中心將持續配合教育部措施與其他各網路中心共同進行下列之重點任務。

2.2.1 網路管理

為協助網路管理人員掌握網路壅塞及 TopN user，區網中心建置了多部 server 收集各個連線界面、各個連線學校之流量作統計並分析，做為設定相對管理措施之依據，同時也能掌握造成網路各種現象之原因。並建置了：連網機房維運紀錄與溫度監看網站、網路及主要伺服系統運作狀況監看網站，協助網路管理人員確認連網的正常維運，及累積連網問題的處理經驗。

(i) Zabbix 自動監測系統，<https://zabbix.tyc.edu.tw> 針對重要網路設備、機房溫溼度監測、實體及虛擬伺服器的服務效能，利用自動化程序監測。並自行開發 LINE Notify 程式，進行 LINE 即時訊息自動發送警示訊息，讓網管人員及早發現問題並立即處理。

圖 2. 桃園區網 Zabbix 自動監測系統



(ii) 主要連線 MRTG 流量及 TopN 使用流量統計及應用分析

區網的 MRTG 流量監看網站及 TopN 使用流量統計網站，協助網管人員監看：桃園區連線學校專線的 MRTG 流量、TANET 出國專線流量、TANET 骨幹各區網中心流量，及桃園區 ISP 互連幹線流量。而 Top-N user 流量統計網站則協助網管人員掌握：每日之 Top-N user、每月之 TopN user、TopN user 及各應用軟體之流量統計。

表 2 Cacti、MRTG 流量統計

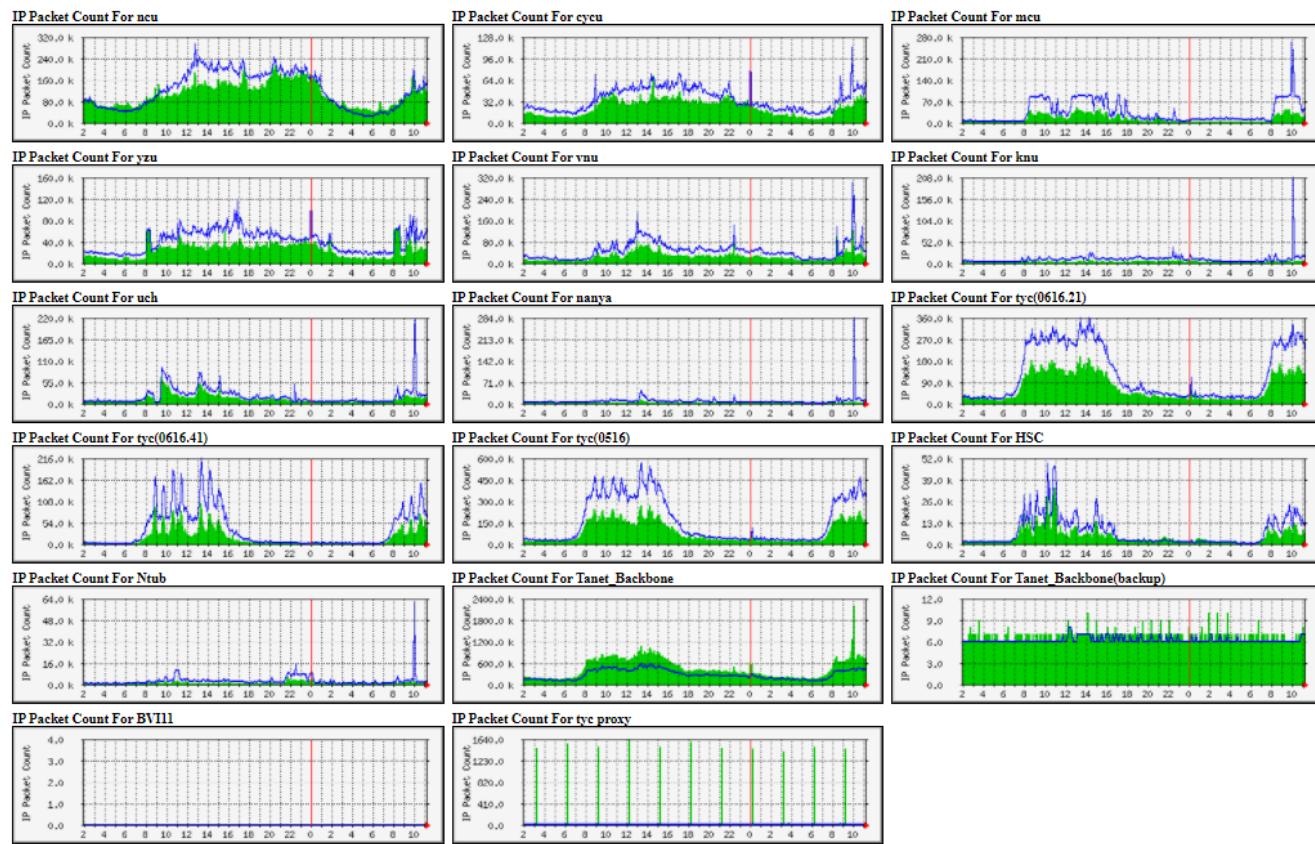
| | |
|-------------------------|---|
| 1. 每日 Top-N user 流量統計 | https://nreport.tyrc.edu.tw/ (須用帳號密碼登入) |
| 2. 每月 TopN user 流量統計 | https://nreport.tyrc.edu.tw/ |
| 3. TopN user 及各連網應用流量統計 | https://nreport.tyrc.edu.tw/ |

(iii) 網路及主要伺服系統運作狀況監看

區網中心透過依據：區網骨幹 router 的 ICMP response，DNS server 的 dig 查詢回應，wget www 服務網站，及各連線學校網路運作狀況(圖 3)，協助網路管理人員確保聯網及主要服務的正常提供。

圖 3. 各連線學校網路運作狀況

tyrc-packet-mrtg



2.2.2 IPv6 網路建置

配合教育部進行 IPv6 連網的建置計劃，桃園區網已完成桃園區網與下連單位進行跨區的 IPv6 連網環境建置與測試(表 3). 其間，我們也紀錄了 IPv6 routing /DHCP 服務，IPv6 DNS serve 的設定與測試經驗，作為開放 IPv6 知識庫的基礎。2024 年已全數完成 100%連線學校導入 IPv6 環境。

表 3 桃園區網導入 IPv6 之學校與單位

| 單位 | 網段 | 支援 IPv6 |
|--------|--------------------|---------|
| 桃園區網 | 2001:288:3000::/48 | OK |
| 國立中央大學 | 2001:288:3001::/48 | OK |
| 國立體育大學 | 2001:288:3002::/48 | OK |
| 中原大學 | 2001:288:3003::/48 | OK |
| 元智大學 | 2001:288:3004::/48 | OK |
| 銘傳大學 | 2001:288:3005::/48 | OK |
| 健行科技大學 | 2001:288:3006::/48 | OK |

| | | |
|----------------|--------------------|----|
| 萬能科技大學 | 2001:288:3007::/48 | OK |
| 開南大學 | 2001:288:3008::/48 | OK |
| 南亞技術學院 | 2001:288:3009::/48 | OK |
| 中央警察大學 | 2001:288:300A::/48 | OK |
| 國防大學 | 2001:288:300B::/48 | OK |
| 新生醫專 | 2001:288:300C::/48 | OK |
| 陸軍專科學校 | 2001:288:300E::/48 | OK |
| 私立大華高級中學 | 2001:288:3010::/48 | OK |
| 私立復旦高級中學 | 2001:288:3011::/48 | OK |
| 國立臺北科技大學附屬桃園農工 | 2001:288:3013::/48 | OK |
| 私立新興高級中學 | 2001:288:3014::/48 | OK |
| 私立治平高級中學 | 2001:288:3015::/48 | OK |
| 私立育達高級中學 | 2001:288:3016::/48 | OK |
| 私立至善高級工商職業學校 | 2001:288:3017::/48 | OK |
| 私立永平高級工商職業學校 | 2001:288:301D::/48 | OK |
| 國立中壢高級中學 | 2001:288:301E::/48 | OK |
| 私立清華高級中學 | 2001:288:301F::/48 | OK |
| 私立大興高級中學 | 2001:288:3020::/48 | OK |
| 私立啟英高級中學 | 2001:288:3021::/48 | OK |
| 私立六和高及中學 | 2001:288:3022::/48 | OK |
| 私立成功高級工商職業學校 | 2001:288:3023::/48 | OK |
| 私立振聲高級中學 | 2001:288:3025::/48 | OK |
| 私立方曙高級商工職業學校 | 2001:288:3028::/48 | |
| 核能研究所 | 2001:288:302A::/48 | OK |
| 國防大學理工學院 | 2001:288:302B::/48 | OK |
| 北區教育雲 | 2001:288:3100::/48 | OK |

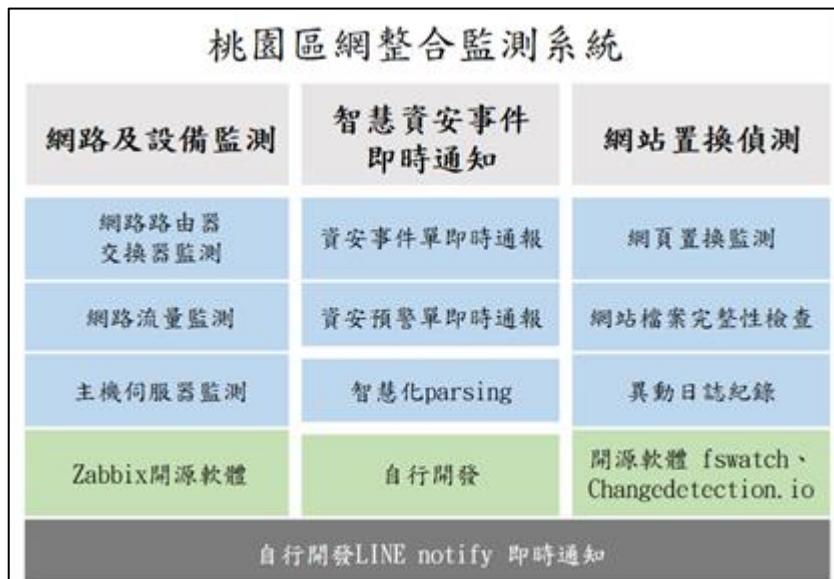
| | | |
|---------------|--------------------|----|
| 桃園市網 | 2001:288:3200::/39 | OK |
| 連江縣網 | 2001:288:3600::/39 | OK |
| 金門縣網 | 2001:288:3400::/39 | OK |
| 國立臺北商業大學-資網中心 | 2001:288:302c::/48 | OK |

| 連線單位 | 單位數 | 完成 IPv6 單位數 | 未完成 IPv6 單位數 | 完成 IPv6 比率 |
|-------|-----|----------------|-----------------|------------------|
| 縣市網中心 | 3 | 3 | | 100% |
| 大專院校 | 16 | 16 | | 100% |
| 高中職 | 19 | 19 | | 100% |
| 總計 | 38 | 38 | | 100% |

2.2.3 整合監測系統結合即時告警

桃園區網為隨時監測區網及連線學校的網路設備和資源，即時接獲資安事件通報及處理，隨時掌控網站服務是否正常，建置整合監測系統結合即時告警。智慧資安事件即時通知平台接收到資安事件及資安預警事件時，使用智慧化 parsing 識別資安事件和相對應處理的連線學校。利用電子郵件及 LINE 即時通知給區網連線學校應變處理。

圖 5 整合監測系統架構



智慧資安事件即時通知平台接收到資安事件及資安預警事件時，使用智慧化 parsing 識別

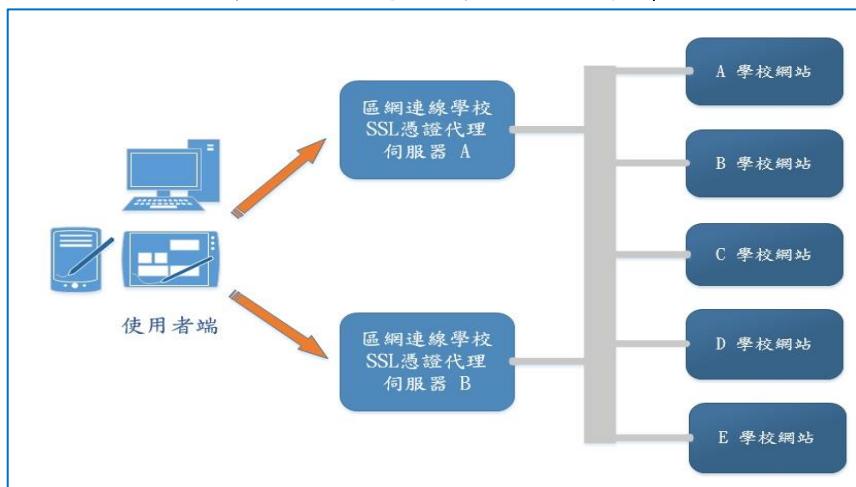
資安事件和相對應處理的連線學校。利用電子郵件及 LINE 即時通知給區網連線學校應變處理。

2.2.4 HTTPS 憑證代理服務

教育部 110 年 6 月 29 日臺灣學術網路(TANet)技術小組第 96 次會議決議，各級學校網站應導入 HTTPS。桃園區網協助連線學校導入 HTTPS 過程中，大專院校有比高中職較多的人力與資源，而公立國高中學校有市網中心協助，但私立高中職學校網站升級 HTTPS 有其困難度。原因包含部分私立高中職資訊經費拮据，硬體平台使用多年，機器老舊。學校資訊組長一人負責全校所有網路及資訊工作，工作繁重，網站及應用系統無廠商維護。

桃園區網中心為了協助高中職學校網站導入 HTTPS，利用開源軟體 NGINX 的反向代理特性，達成後端網站伺服器的 SSL 憑證代理。從 110 年起總計完成 12 所學校共 21 個學校網站使用區網憑證代理服務，區網憑證代理伺服器使用 TLSv1.2，TLSv1.3，以及 HSTS，協助連線學校網站取得 A+ 安全性評等。

圖 6 HTTPS 憑證代理伺服器架構



導入過程中，學校網站在完全不需要更動原網站設定及網站程式碼下，順利導入 HTTPS。部分學校網站也能在區網協助下，變動幅度甚小之後完成導入 HTTPS。變動部分由桃園區網中心與學校資訊組長共同檢視網頁混合內容，以相對連結 URL 取代絕對連結 URL，修改網站設定及調整網站程式以導入 HTTPS。

2.2.5 網站應用程式弱點監測

桃園區域網路中心每年提供 2 次（上半年及下半年）資安檢測服務，使用 Nessus Professional、HCL AppScan 做為檢測工具。區網皆會提供中高風險的改善建議，並定期追蹤申請單位是否針對弱點結果修正，修正後會再次以 OpenVAS 執行複掃以確保弱點是否已修復。113 年度，全面對所有連線學校官網弱掃及個別申請弱掃共計 36 所學校，系統弱點掃瞄 2415 個主機，網頁弱點掃描 729 個網站。

112 年度開設「弱點掃描與檢測實務」、「如何看懂弱掃報告」、「網站應用程式常見弱點解析」等三門教育訓練，共 18 小時。113 年度開設「系統與網站攻防演練」、「事件調查與分析實務」、「滲透測試-從技術到實作」等三門教育訓練，共 18 小時，桃園區域網路中心藉由教育訓練著手，培訓連線學校夥伴如何修補主機弱點。

2.2.6 資安維運中心(SOC)建置

桃園區網端與 TANet 骨幹間進行流量之 Layer 7 分析，提供入侵偵測、阻擋，並與 ASOC 合作建置 Sourcefire IPS 入侵防禦設備，提供入侵事件通告/回報系統，降低問題事件。

2.3 辦理資訊推廣活動

區網中心每年均舉辦多場的網路技術、資訊安全研討會，並將課程教材上網。未來，也將依據區網連線學校回饋的需求主題，規畫研討課程：如 IPv6、網路技術及管理、OpenSource 軟體、社交工程、網路安全防護、智慧財產權、綠色機房、AI、IoT、電腦鑑識、網路流量監控、網路攻擊防禦(軟硬體)等，並規劃技術層面的實作技術教學、校園無線化網路管理。

2.4 創新服務

2.4.1 無線漫遊向上集中

桃園區網連線學校中，許多學校人力資源及資訊經費有限，要做到全面導入 eduroam 無線漫遊，有其執行上的困難。因此為了解決各校不容易自行建置 eduroam 無線漫遊的問題，桃園區網中心 113 年度建置無線漫遊向上集中系統，成為臺灣學術網路第一所提供無線漫遊向上集中的區網中心。希望連線學校能藉由使用區網漫遊向上集中系統，能以最快的時間和最簡化的設定完成導入 eduroam 無線漫遊。無線漫遊向上集中系統提供了無線漫遊介接服務，分為單向和雙向兩種類型。。

無線漫遊向上集中系統簡化過去連線學校需要繁複的設定，各校僅需下載 LDAP 憑證，設定各校 AP Controller 設定。後續認證平台與漫遊中心 OPEN VPN 憑證及與漫遊中心介接設定，皆由桃園區網建置。自建 eduroam 與 向上集中 eduroam 工作項目比較表如下。

圖 7. 桃園區網無線漫遊向上集中優點比較表

| 項目 | 自建 eduroam 伺服器 | 向上集中 eduroam 伺服器 |
|------------------|------------------------------------|---|
| 漫遊中心 OPEN VPN 憑證 | 自行申請 | 免申請 由桃園區網管理  |
| 網域SSL憑證 | 自行申請 | 免申請 由桃園區網管理  |
| Google LDAP憑證 | 自行申請每三年更換 | 自行申請每三年更換 |
| 硬體維護 | 自行維護 | 由桃園區網維護  |
| 安全性 | 佳 | 優  |
| 需要Linux技術 | 進階 | 由桃園區網提供  |
| 無線網路設備支援度 | 需支援 IEEE802.1X 驗證，無法支援此驗證模式，僅可單向驗證 | |

過去一所學校導入 eduroam，從規劃、建置 Radius Server、與無線漫遊中心介接及設定 AP 控制器，動輒要數天到數禮拜才能完成。藉由桃園區網迅速且便利的無線漫遊向上集中系統，大幅縮短各校完成導入 eduroam 無線漫遊的時間。目前累計已完成 3 所大學及 5 所高中職完成 eduroam 向上集中。

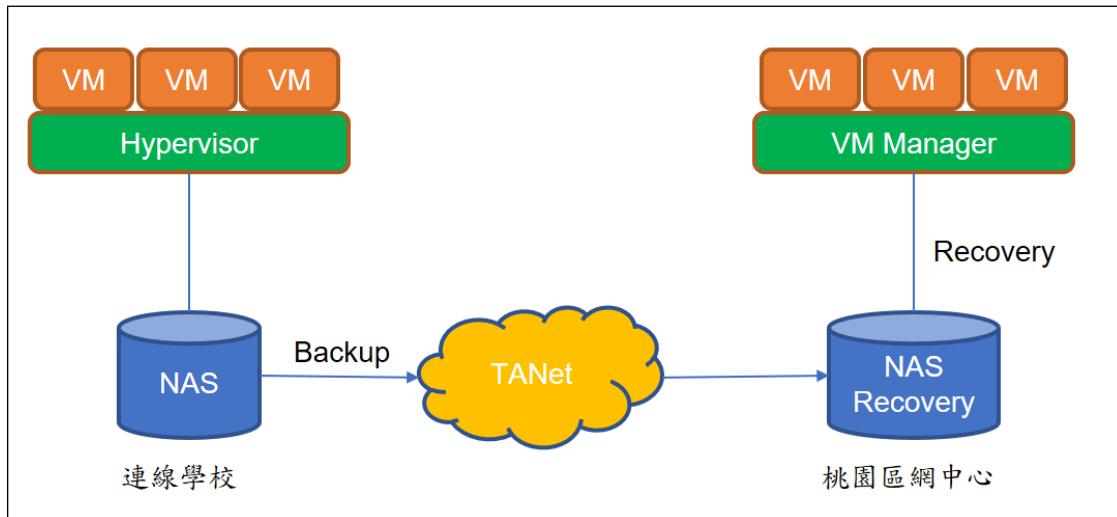
2.4.2 異地備份、異地備援服務

異地備份是推動資訊安全管理的重要工作之一，為提供連線單位更可靠之服務，以面對災難後，復原業務運行。然而因進行異地備份租賃機房等費用昂貴，花蓮區網中心(國立東華大學)與桃園區網中心(國立中央大學)合作平等互惠使用對方儲存空間為異地備份，111/9/19 與東華大學簽訂異地備份合作備忘錄，並完成技術驗證作業。

為確保重要資料之機密性，雙方請轄下連線單位各自事先加密以確保資料之隱密性。目前已全面開放桃園區網連線學校申請異地備份服務，異地備份空間額度，高中職：2TB，大專院校：3TB，縣市教育網路中心：4TB。目前已協助 10 所高中職、4 所大學、1 所縣市網路中心完成異地備份至桃園區網中心，並以自動排程備份到 100 公里外的花蓮區網中心。

2023 年 9 月升級為異地備援服務，桃園區網中心全面提供連線學校申請使用。如連線學校重要系統無法使用時，可以在桃園區網機房恢復系統正常運作，讓連線學校重要服務不致中斷。

圖 8. 桃園區網連線學校異地備援架構



桃園區網已完成 17 所連線學校的異地備份，112 年至 113 年已完成六和高中、長庚科技大學、陸軍專科學校、育達高中、新興高中、啟英高中等 6 所學校實際演練異地備援至桃園區網。透過實際演練，各學校可以模擬當學校端資訊系統失效的情況，測試由區網異地備援系統接替服務的能力。確保在實際災難發生時，服務能夠順利轉移和持續運作，讓連線學校可以有效的應對潛在風險，也確保資料在任何情況下都能得到妥善保護。後續並藉由實際演練經驗，桃園區網、陸軍專科學校、六和高中共同撰寫異地備援計畫及備援 SOP 提供其他連線學校參考使用。

2.4.3 DNS 向上集中

110 年桃園區網為了提升 DNS 的安全，與桃園市網中心合作，主動協助桃園市私立高中職學校 DNS 伺服器向上集中。從 110 年 07 月 30 日開始，到 111 年 3 月 28 日完成最後兩所高中 DNS 向上集中，在 9 個月內完成全部 14 所私立高中職 DNS 向上集中作業。DNS 向上集中優點，減少高中職學校建置管理 DNS 系統維護成本，完成 DNSSEC 簽署及 RPZ 設定，增加了 DNS 服務安全性。減少 14 所學校共 16 台 DNS 伺服器的能源消耗，達成環保節能減碳。

| 連線單位 | 單位數 | DNS 已更新 | DNS 最新版本比率 |
|-------|-----|---------|------------|
| 縣市網中心 | 3 | 3 | 100% |
| 大專院校 | 14 | 14 | 100% |
| 高中職 | 18 | 全部向上集中 | 100% |

2.4.4 協助優化資訊服務，加強傳輸存取品質

隨著網路無遠弗屆的優勢，線上學習與教學平台的網路互動隨之蓬勃發展，當數位資訊的交流越來越頻繁，對於網路頻寬的要求亦隨之增加，加上因受新冠肺炎（COVID-19）疫情衝擊，全國各校迫切需要實施遠距教學。然而，既有的網路環境面臨頻寬不足以因應所有學生同時連線的需求，有鑑於此，為了提高遠距教學的教學品質，同時增進數位學習及科技教育的推動，以奠定臺灣在國際間科技優勢的長遠基礎，桃園區網於金門縣教育網路中心、連江縣教育網路中心及本區網中心建置「內容傳遞網路服務」，以舒緩各級學校因實施數位或遠距教學之頻寬需求，及作為未來常態提供網路教學所需的頻寬環境。

內容傳遞網路服務是一種在網際網路上透過建立分散式的伺服器群就近與使用者建立連線，以便更快速地將音樂、圖片、影片、應用程式及其他檔案傳送給使用者，減少相關資料傳輸之延遲時間，並大幅節省骨幹網路的頻寬使用，藉此達到提供高效能、可擴展性及低成本的網路服務之目的。

內容傳遞網路服務之所以能大幅節省骨幹網路頻寬的原因在於，當只有一台伺服器（以下稱為「原站」）提供網站服務時，所有的流量都必須連線到原站才能取得所需的資源，而透過內容傳遞網路服務的機制來建立分散式的伺服器群，每一台伺服器各自建立暫存的資料內容，如此一來當使用者有需求時，可以就近透過最近的一台伺服器取得所需的資源，而毋須每次都去訪問原站，除了瀏覽網站的頻寬流量，並大幅減少使用者取得資源所需耗費的時間。

內容傳遞網路服務更可透過伺服器群來達到異地備援的效果，當某台伺服器發生故障時，系統可迅速調用鄰近地區其他伺服器來提供服務，進而達到接近 100% 的可靠度，這個機制同時可以防範小規模的 DDoS 攻擊。

桃園區網 111 年於金門縣教育網路中心及連江縣教育網路中心所建置 CDN Edge 節點，112 年延續教育部計劃，於本區網中心機房建置內容傳遞網路服務備援節點，並於建置完成後則加入教育部管理中心統一管理，透過金門縣教育網路中心、連江縣網路中心及本區網中心內容傳

遞網路服務伺服器群的部署建置，期望達成降低 TANet 骨幹網路流量、協助優化資訊服務、加強傳輸存取品質以及增加備援機制等目標，以有效提升其學術網路的整體服務品質。

2.4.5 教育雲北區雲端資料中心

依據教育部「教育雲端應用及平台服務推動計畫」，成立教育部本部及北、中、南四區教育雲端資料中心，以提供教育雲之基礎建設。中央大學除擔負桃園區網中心維運重任之外，也擔任教育雲北區資料中心(以下簡稱本資料中心)。區網中心目前提供三百多所各級學校介接全球 Internet 網際網路，包括：桃園市、金門縣及連江縣三個國中小教育網路中心及多所大專院校、學研單位及高中職等學校。而本資料中心則以 IaaS (Infrastructure as a Service)服務為主，提供虛擬機的租用，整合現有之雲端運算資源，提供給北區師生所用。

教育部教育雲端應用及平台服務推動計畫，本計畫是以維運一個雲端資料中心，提供一個安全、可靠、隨即可用的 IaaS 的服務。透過雲平台的基礎建設，提供線上學習、教學資源、學習管理、學習社群等多項服務。

圖 8. 教育雲服務整合與開發架構



本資料中心於民國 102 年建置完成後，其服務對象為非營利之全國性教育、學術研究相關應用服務，以 10 Gbps 頻寬連接至 TANet 骨幹網路。本資料中心以 IaaS 服務為主，提供虛擬機相關資源，採預建虛擬機映像檔的方式-隨申請隨用不需要安裝的方式，提供 Linux, FreeBSD 及 Windows 等系統。本資料中心可提供的資源包括：虛擬機、vCPU、記憶體、儲存空間、實體 IP 位址，且支援 IPv6。

硬體的配置-電力，網路及儲存裝置均支援 HA 的功能，避免意外發生時導致服務中斷。系統架構以兩台核心交換器為中心，往上透過防火牆與桃園區網核心交換器 ASR 介接，兩台核心交換器提供 Server Farm 的實體主機兩套具備援的網路，另有一台負載平衡器接至核心交換器提供網路服務的負載平衡。Server Farm 的每台伺服器均備有兩張 HBA 卡分接至兩台 SAN Switch，SAN Switch 後端則是兩台儲存虛擬化設備互為備援，最後才接到實際的儲存設備。在這樣的架構下，不論在網路、線路、儲存都達到高可用性的需求。

在伺服器的部份，每台主機於 109 年提昇網路埠之頻寬，並增加兩台 Switch，可提供 40G 的流量，包括主機管理、Heartbeat 及資料流量，另外一個 Out-of-band 管理 port 接到內部管理用的交換器，除此之外，於 109 年增加由教育部至北區雲端中心 10G 內網專線，以及增加

IPS/ATP 資安設備，於防火牆跟 Switch 之間。其中，內部管理用的交換器銜接所有的網路設備、伺服器、SAN Switch 及儲存裝置，由於是內部管理用途，未在圖上呈現。核心交換器提供兩條 10G 線路至負載平衡器，對外也是用兩條 10G 的網路連接至防火牆。負載平衡器及防火牆至核心交換器間都採用 802.3ad 的標準，兼具頻寬的增加及線路的備援。防火牆到區網 Router (ASR) 間則以 10G 網路介接，透過 ASR 接至 TANet 骨幹。

| 服務系統名稱 | vm數量 | vCPU | vRAM | vHD |
|----------------------|-----------|------------|----------------|------------------|
| TANet_VoIP | 3 | 12 | 48 | 240 |
| 因材網 | 1 | 8 | 16 | 400 |
| 字音字形網 | 1 | 8 | 16 | 160 |
| 英語線上學習平台 | 2 | 48 | 128 | 3048 |
| 教育單位弱點檢測平台 | 1 | 8 | 16 | 100 |
| 教育媒體影音 | 6 | 24 | 48 | 11160 |
| 教育體系單一帳號驗證授權平臺 | 10 | 96 | 220 | 950 |
| 微積分題庫 | 1 | 4 | 8 | 100 |
| 數學小學堂系統 | 3 | 14 | 28 | 1304 |
| 磨課師 | 2 | 16 | 32 | 40 |
| 體育署_體育雲-全民運動資訊系統 | 13 | 60 | 120 | 3948 |
| 體育署_體育雲-全民運動資訊系統報名網站 | 9 | 40 | 80 | 900 |
| 總計 | 52 | 338 | 760(GB) | 21.83(TB) |

2.5 未來工作及預期效益

114 年朝網路高可用性及提升數位韌性兩大目標進行，網路高可用性透過整合監測系統自動偵測，即時告警，並加強 BCP 演練及維運應變計畫，網路可用率達 99.99%。提升數位韌性將藉由事前預防、事中調查，事後復原方向努力，其中事後復原將定期測試異地備份資料，確保其可用性。定期檢查測試回復程序，並定期協助連線學校演練，使用異地備份資料還原，目標為 47% 學校使用，4 所學校完成異地備援演練。

明年度網路管理及資訊安全預計工作如下：

A. 網路管理

- 持續機房維運建設(電力、空調)，維持良好網路運作，維持骨幹基礎環境之妥善率及連線學校之網路妥善率達 99.99% 以上。
- 每年辦理 2 場管理及技術委員會會議，宣導教育部相關政策，以促進區縣網中心與連線單位間有效地協調及合作。
- 邀請 4 個連線單位輪流分享該校網路管理經驗以達到技術與經驗之交流提升區縣網中心與連線單位的技術與經驗交流。
- 網路流量監控。
- 提供 Google Global Cache 服務。

B. 資訊安全

- 每年完成 4 所學校異地備援演練，並持續推動區網 47% 連線學校使用異地備援服務。
- 提供區網 IPS log 分析與攻擊偵測。
- 超量攻擊之預警與阻擋。

- 協助連線學校降低疑似侵害著作權之問題事件。
- 協助連線學校降低不當資訊的流竄、網路攻擊事件之發生，以提昇網路使用效率。
- 提供區域網路中心及連線學校網路實體環境資安防護機制，並全面對連線學校進行網站掃描及系統弱點掃描。持續協助連線學校進行網站掃描、健檢、演練等資安相關服務。
- 配合 TACERT 執行資安相關資通安全通報應變作業，並協助連線學校資安事件因應處理。
- 每年提供 2 次資安檢測服務，連線單位除上述時間，如有臨時需資安檢測可隨時向桃園區域網路中心申請。

C. 雲端服務

- 加強教育雲服務，提供建置私有雲及教育雲服務之經驗分享/推廣。
- 提供連線學校雲端伺服器相關服務，建置各校伺服器健檢系統及各連線單位連線狀態檢測系統。

D. 辦理教育訓練及推廣活動

- 預計辦理 7 場教育訓練，包含網路管理及技術、資訊安全、雲端應用、異常流量分析及偵測、IPv6 推廣等相關議題課程，並規劃實作的 workshop 課程，強調動手做來加強學習。

2.6 114 年度 KPI

| 項次 | 未來營運方針 | 目標值 |
|----|---|-----------------------------|
| 1 | 全年電路服務妥善率 | 99. 99% |
| 2 | 召開區域網路中心管理會議，邀請連線單位分享該校網路管理經驗。 | 召開 2 次會議，出席率 90% |
| 3 | 辦理網路管理及資訊安全教育訓練，課程實質效益分析，50%以上課程需進行前測與後測。 | 辦理 7 場，後測進步平均達 20%。 |
| 4 | 協助連線學校進行弱點掃描、網站網頁檢測等資安服務 | 至少 30 所 |
| 5 | 提供離島縣市教育網路中心網路管理、資安研習、巡檢網路機房環境或技術支援服務。 | 至少 1 次 |
| 6 | 提供連線學校資安巡迴服務。 | 至少 3 次 |
| 7 | 異地備援服務 | 47% 連線學校使用，每年完成 4 所學校異地備援演練 |

3 經費需求

3.1 專任計畫人員任務

| 網管人員(1位)的任務與績效 |
|------------------------------|
| 維護區網網路正常連線，線路異常排除 |
| 通訊網路設備管理 |
| 建置網路管理系統，DNS 及 WWW server 管理 |
| 機房及基礎環境(電力, 空調, 溫濕度, 消防設備)維護 |
| 辦理網路管理技術研討會, 臨時交辦事項 |

| 資安人員(1位)的任務與績效 |
|----------------------------|
| 資安通報審核及演練，資安事件處理 |
| 異常流量 IP 偵測及處理 |
| 協助 ISO27001 資安認證, 個資保護系統維護 |
| 弱點掃描，網頁檢測及追蹤處理 |
| 辦理資安研討會，臨時交辦事項 |

| 雲端管理人員(1位)的任務與績效 |
|--------------------------------------|
| 配合教育部資安政策，定期修改防火牆相關設定 |
| 協助臨時性防火牆調度支援教育部，以及備用機器歸還事宜 |
| 維護北區雲端資料中心儲存空間、網路設備、運算主機正常運作，並處理異常排除 |
| 建置北區雲端資料中心遠端連線設備權限設定並定期更新 |

3.2 計畫經費說明

網管人員 1 名；資安管理人員 1 名；北區教育雲雲端資料中心管理人員 1 名。詳列於『臺灣學術網路(TANet)桃園區域網路中心 114 年度基礎維運與資安人員計畫』經費申請表。

基本營運(教育部補助經常門) 詳見『臺灣學術網路(TANet)桃園區域網路中心 114 年度基礎維運與資安人員計畫』經費申請表。

| 項目 | 預估經費 | 營運規劃 |
|-----|-----------|------------------------------|
| 人事費 | 2,220,803 | 三名專任助理，分別負責網路管理、資訊安全、教育雲。 |
| 業務費 | 1,229,197 | |
| 設備費 | 1,410,000 | 持續建置異地備援系統，並預計採用不可變快照防範勒索病毒。 |
| 合計 | 4,860,000 | |