

臺中 區網路中心

「104 年度 TANet 區域網路中心基礎維運
及資安人員計畫」

103 年 12 月 23 日

【目 錄】

壹、計畫基本項目	1
一、計畫期程：104.1.1~104.12.31	1
二、計畫執行單位：中興大學計算機及資訊網路中心	1
貳、區域網路中心基本維運計畫執行內容	1
一、現況說明(含網路架構圖)	1
二、工作內容	5
三、辦理資訊推廣活動	8
四、網路應用特色服務	8
五、預期效益	9
參、經費需求	10
一、人事費（網管、資安、教育雲管理各 1 員；兼任助理 1 名）	10
二、基本營運（教育部補助經常門）	10

壹、計畫基本項目

一、計畫期程：104.1.1~104.12.31

二、計畫執行單位：中興大學計算機及資訊網路中心

貳、區域網路中心基本維運計畫執行內容

一、現況說明(含網路架構圖)

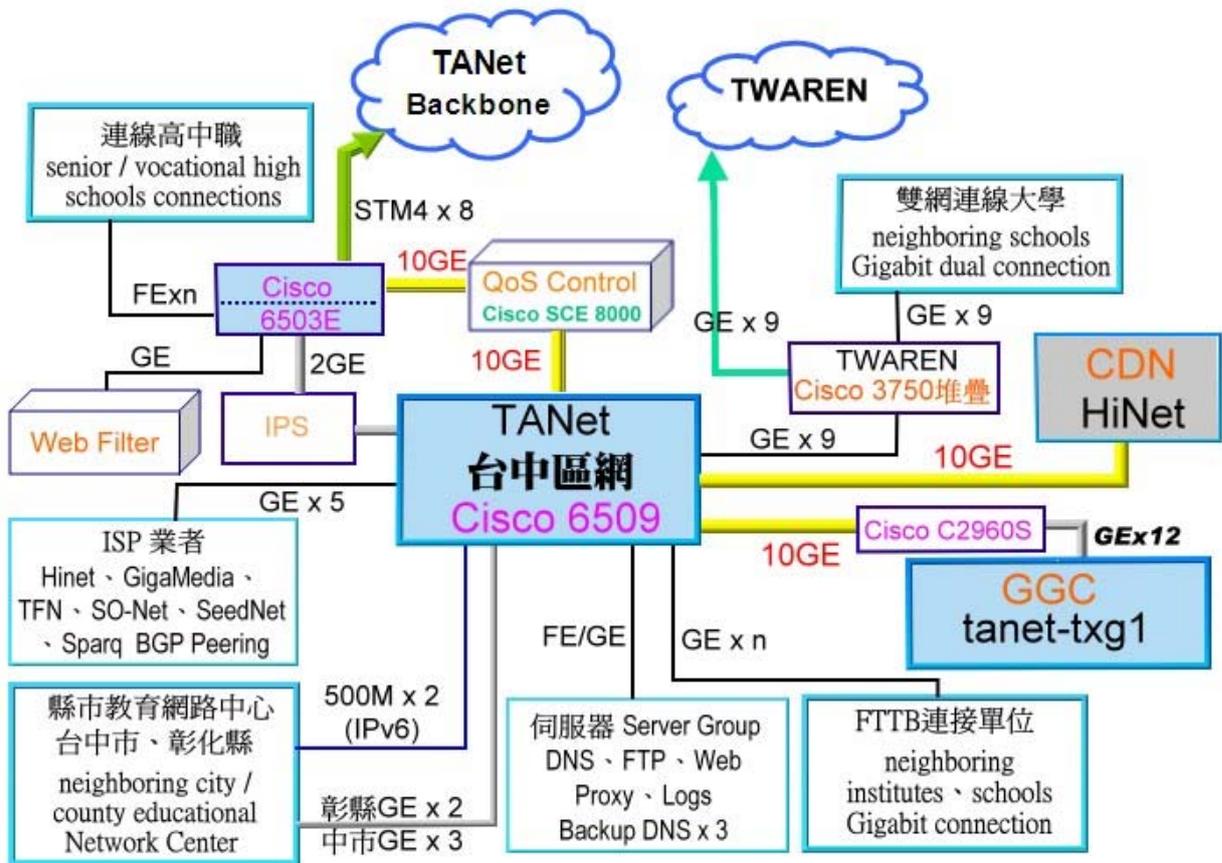
(一)、目前工作、任務及網路連線情形

目前本中心透過 TWAREN 5 Gbps 的頻寬，以都會型網路架構連接至骨幹，並與國內多家網路業者(Hinet、SeedNet、和網寬頻、APOL、TFN、SO-Net、速博)以 Gigabit、FastEthernet 等專線作多點互連，快速交換網路資訊，是 TAnet 骨幹中部地區重要的一環。本中心下連臺中直轄市和彰化縣兩個教育網路中心，共同推動中小學資訊網路，提供中部地區學術研究單位之連線、技術諮詢以及資安管控等相關服務。

基於分工原則，縣市中小學分別以 ADSL、光纖與其直屬縣市網路中心連接，本中心則提供各縣市網路中心及中部縣市之高中職以上學校直接連線，目前有縣(市)網、大專院校、高中職、醫療機構等 49 個單位與本中心連線，其中臺中直轄市和彰化縣網路中心下計有五百多所中小學。此外，位於南投縣境內的南開科技大學和其他 4 所高中職目前仍與本校維持直接連線。在教育部新建置的新世代骨幹網路下，本區網中心全力推動與各學術單位銜接，以提升網路頻寬，加強管理功能，提供最好的網路環境給境內師生使用。102 年 6 月與 Google 公司合作，建置台中區網 Google Global Cache(GGC)服務，大幅提升下游連線單位存取影音資料之品質與速度，並有效減低出口頻寬壅塞的窘境。103 年 1 月則與 HiNet 合作建置 Content Delivery Network(CDN)，加快臺灣學術網路各使用單位存取 HiChannel 平台的速度。

103 年 10 月將臺中區網骨幹頻寬由 4Gb 擴充為 5Gb，以暫時解決骨幹出口日益雍塞的問題。

(二)、區網中心網路架構圖



(三)、建置及管理的網路服務系統及設備

本中心建置及管理的網路服務系統均提供全年無休的運作以供本地區連線單位使用，計有以下：

1. Core Switch * 1、Switch * 1

domain name : tbb.tcrc.edu.tw、6503E

ip address : 140.128.248.201, 140.128.251.221

model: catalyst 6509 sup720 (教育部骨幹及區網使用), catalyst 6503E sup720(高中職資安防護)

➔提供 Fast Ethernet 100Mb 及 Gigabit 連線

2. Domain Name Server * 3

domain name: ns1.tcrc.edu.tw, ns2.tcrc.edu.tw, ns3.tcrc.edu.tw

ip address :

ns1: 163.28.82.1, 2001:288:5000:3::1

ns2: 163.28.82.5, 2001:288:5000:3::5

ns3: 163.28.80.3, 2001:288:5000:1::3

model: VMware 虛擬機器 FreeBSD*2

VMware 虛擬機器 Fedora*1

→提供 DNS 查詢服務

3. FTP server * 1

domain name: ftp.tcrc.edu.tw

ip address; 163.28.80.21 , 2001:288:5000:1::21/64

model: IBM eServer xSeries 255

→提供 public domain 軟體

4. Cisco 管理伺服器 * 1、Cisco SCE * 1

domain name : 無

ip address :

model:UCS C210 M2 , Cisco SCE 8000

→位於區網骨幹出口，提供連線單位流量管制報表、流量管控服務

5. Log server* 1

domain name: cachelog.tcrc.edu.tw

ip address: 163.28.82.3.

model: PC Pentium 4 1.7GHz, Fedora core 4

→提供網管統計資料及流量分析

6. MRTG * 1(兼作 WWW server)

Domain name: www.tcrc.edu.tw

ip addr: 163.28.82.8, 2001:288:5000:3::8

Model: PC Pentium III, Linux

→提供及時流量圖、區網中心網站及資料庫

7. Nettracker * 1

Domain name: nfa.tcrc.edu.tw

Ip addr: 163.28.82.201

model: IBM eServer xSeries 255

→提供即時與歷史流量統計

8. Proxy server * 1

domain name: cache.tcrc.edu.tw

ip address: 163.28.80.40:3128, 2001:288:5000:1::40

model: Network Appliance Netcache C6100

→提供下游 proxy mode service

9. SIP Server* 1

Domain name: sipv6.tcrc.edu.tw

IP addr: 163.28.82.34, 2001:288:5000:4::34

Model: PC pentium 4

→提供高中職網路電話服務

10. Tipping Point (IDS 入侵偵測系統)*1，Sawmill(報表系統) * 1

domain name：無

ip address：163.28.83.1，163.28.83.2

model: TP600E

→提供連線高中職入侵偵測服務

11. 弱點掃描主機*2，排程系統與報表系統主機*1

domain name： waps.tcrc.edu.tw

ip address：163.28.82.116；163.28.80.117、163.28.82.117

model: 1U 機架式伺服器(Server 2008，內含成大所開發之網站應用程式弱點檢測系統)

→提供連線單位網站應用程式弱點掃描服務

→103 年 8 月起新增網站應用程式弱點掃描手持式裝置版服務

12. 虛擬主機伺服器 * 2

domain name:

ip address：163.28.80.4、163.28.80.6

model: IBM system x3455 * 2

VMware vSphere 4 * 1

→提供區網伺服器和連線單位虛擬主機承載服務

13. 網路氣象台簡訊發送機* 1

Domain name:

IP addr: 163.28.80.88

Model: Linux OS

→配合網路氣象台提供異常流量簡訊發送服務

14. 教育機構防洩漏個資掃瞄平台* 1

Domain name: piscan.tcrc.edu.tw

IP addr: 163.28.80.122

Model: VMware 虛擬機器 Windows 7，內含成大開發之防洩漏個資掃瞄系統

→提供各連線教育單位防洩漏個資掃瞄服務

→103 年 10 月起新增防洩漏個資掃瞄手持式裝置版服務

15. Google Global Cache 主機群

Domain name: 無

IPv4 Subnet: 163.28.83.128/26

IPv6 Subnet: 2001:288:5000:7::/64

Model: Dell S720 x 6

→提供連線單位 Google 網頁及影音視訊服務

16. HiNet Content Delivery Network 主機群

Domain name: 無

IPv4 Subnet: 163.28.83.112/28

Model: Dell S720 x 2

→提供 TAnet 所有連線單位 HiChannel 網頁及影音視訊服務

二、工作內容(配合教育部資訊及科技教育司)

根據近幾年的統計，TAnet 使用至今所呈現之問題，主要仍然有：廣告信件、智慧財產權之侵害、駭客入侵、病毒肆虐、網路濫用導致壅塞、不當資訊之流竄、管理欠嚴謹...等。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以下之重點任務，並戮力執行。

(一)、網路管理

1. 網路使用及流量(含 IPv6)統計分析

為了能掌握網路壅塞及不當資訊流量之即時狀況，本中心專設伺服器(使用 Nettracker、Genie ATM)以收集各個連線界面和各大單位使用者之流量，進行統計分析，作為設定各種管理措施之依據，同時也能掌握造成網路各種現象之原因。

工作範圍：① 對各連接專線界面(校際、區網各大出口)做流量統計(含 IPv6)
② 統計前 100 大使用者(IP)
③ 分析各種應用軟體之使用狀況
④ 做每日、週、月、年之網路流量統計分析
⑤ 建置、監測連線單位定期電路及各主要伺服器主機的 MRTG 流量圖 (網址：<http://www.tcrc.edu.tw/flowmrtg.html>)

2. 機房監控與管理

工作範圍：① 本中心電腦機房和辦公場所已於 97.01.25 通過 SGS 公司第三方驗證，已取得 ISO 27001:2005 SOA1.1 之證照。
98.12.18 通過教育體系第三方驗證(驗證範圍：機房整體維運及一項核心業務)
② 102.12.18 通過教育體系第二循環的第三方『追查稽核』驗證，驗證範圍：計資中心及台中區網中心網路骨幹管理、伺服器主機管理、校務系統維運管理及機房維運管理。本年底將進行第三循環的教育體系第三方驗證
③ 本中心機房目前建有環境監控系統(電力、溫溼度)以及極

早期火災預警系統。另於 101.10.24 新建完成自動滅火系統。以上系統持續運作監控中

- ④ 配合教育雲中部資料中心之建置，將於 104 年 2 月底前，完成機房環境優化工程，將建置冷熱通道及機櫃電源監控裝置，以達到更有效率的能源利用及管理。

3. 繼續推動重要服務具 IPv6 Dual Stack 能力

爲了因應 IPv6 的使用與推廣，各項重要服務，如區網骨幹、Web Server、DNS Server 等已經建置完成 IPv4/IPv6 Dual Stack 功能。

- 工作範圍：
- ① 與縣、市網間使用 IPv6 專線、並啓動 OSPF 路由協定
 - ② 啓用區網與連線下游各大學間 IPv6 通道
 - ③ 盡力協助連線單位之 Web、DNS 等 Server 建置 IPv4/IPv6 Dual Stack 功能
 - ④ 調查與統計大專院校及高中職連線單位網路設備支援 IPv6 之現況

4. 加強網路頻寬管理

- 工作範圍：
- ① 101 年 12 月底完成「台中區域網路中心加強網路頻寬管理及資訊安全計畫」，將原先的頻寬管理設備處理能力由 4Gbps 提升爲 10Gbps，並配合教育部政策進行頻寬管理
 - ② 將利用網路頻寬及流量管制設備，針對 TACERT 公佈之『惡意網站威脅來源清單』進行惡意 IP 的阻擋，以降低不當流量的散布。

5. 提供多項降低骨幹流量之代理伺服器服務

- 工作範圍：
- ① 持續提供區網 Proxy Server 服務以加快連線單位讀取國外網頁的速度，並降低區網骨幹的流量。
 - ② 持續提供 GGC 服務。本中心 102 年 6 月配合教育部資訊及科技教育司規劃，與 Google 公司合作，建置並啓用 Google Global Cache 服務，已有效降低 TAnet 骨幹流量雍塞的情形，達成預期目標。本年度將持續提供該項服務。
 - ③ 持續提供 HiNet CDN(Content Delivery Network)服務。爲因應近年來多媒體串流(如 MOD) 流量大幅增加，並有效降低臺中區網與 HiNet 間 BGP peering 流量雍塞的情形，本配合教育部資訊及科技教育司之規劃，於 103 年 1 月與中華電信公司合作，建置並啓用 CDN 服務。本年度將持續這項服務，並觀察其成效。

(二)、網路安全(資通安全)

1. 配合教育部資訊及科技教育司規劃，建立網路安全防範機制

- 工作範圍：
- ① 建立訊息公告鏈結
 - ② 提供各種平台 patch 程式
 - ③ 加強宣導資通安全相關檢測工具系統(如：網站弱點掃描、防洩漏個資掃描)之使用

2. 配合教育部規劃，實踐符合 TANet CERT 台灣學術網路危機處理中心規定之網路安全通報機制

- 工作範圍：
- ① 配合資訊及科技教育司，進行資安通報及演練計畫
 - ② 加強宣導教育機構資安通報平台規定之通報機制
 - ③ 配合資安預警情資(EWA)管理平台進行預警情資的追蹤、稽核、確認與回報。

3. SPAM Mail 檢舉處理機制

Spam mail 造成的原因可能是使用者自行濫用網路、密碼被盜或 mail server、proxy server 的管理不善...等

- 工作範圍：
- ① 檢查 log 並接受連線單位使用者反應，採取適當對策
 - ② 管制沒有存取限制之 mail server 及 proxy server
 - ③ 配合教育部資安政策，貫徹教育機構資安通報機制及區網 Spam mail 回報機制
 - ④ 針對各連線單位被檢舉案件定時提出檢討

4. 智財權檢舉案件追蹤

- 工作範圍：
- ① 確實依據教育部資訊及科技教育司訂定之*台灣學術網路智慧財產權疑似侵權 SOP*處理
 - ② 轉知案件所屬連線單位，並於區網管理委員會中公佈宣導
 - ③ 於每月教育部規定的日期之前，協助連線單位上網填報每一筆疑似侵害智財權檢舉案件的處理情形

5. 提供連線學校相關資通安全技術與事件處理之支援協助

- 工作範圍：
- ① 配合教育部資訊及科技教育司做好資通安全相關工作
 - ② 連線單位發生資安事件並提出協助需求者，盡力協助之
 - ③ 將資通安全教育訓練納入主題式研討會中，預計舉辦 3~5 場資安相關研討會

6. 加強惡意網站威脅 IP 之管理

- 工作範圍：
- ① 針對 TACERT 公佈之『惡意網站威脅來源清單』，除了教育部已在入口進行阻擋的 500 個 IP 之外，將利用網路頻寬及流量管制設備進行其餘漏網 IP 的阻擋

(三)、持續提供連線單位網管相關諮詢、服務與協助

持續提供連線單位網管相關諮詢、服務與協助

- 工作範圍：
- ① 定期召開區網中心管理委員會議(本區網由全體連線單位組成)，完整呈現相關會議資料並提供下載
 - ② 提供連線單位 Proxy server, FTP、DNS server 交換等服務
 - ③ 繼續提供連線單位 SIP/ENUM 交換服務(已支援 IPv6)，提供連線單位網路電話的使用，加強彼此間之技術交流、節約電話費用。目前本區網有 SIP proxy server 2 部(組成 HA 備援架構)，下接 10 所大學 7 所高中職及 1 所文教機構
(104 年度估計約需維護費用 9 萬元整)
 - ④ 提供縣(市)教育網路中心及連線單位技術諮詢並協助規劃良好的網路環境
 - ⑤ 配合教育部完成 40Gbps 骨幹之建置並提供服務
 - ⑥ 繼續提供連線單位流量管控(P2P)服務
 - ⑦ 持續提供 GGC 及 HiNet CDN 服務
 - ⑧ 配合教育部政策，完成教育雲中部資料中心建置及提供相關服務

三、辦理資訊推廣活動

使用網路所造成的種種問題，並不是僅靠少數人的網路技術及各種防範措施可以解決。根本的解決之道應該是以分工合作的方式，讓網路技術與正確的網管觀念互相配合，讓每個連線單位都能正確而安全地管好自己的網路。因此，應加強宣導各種與網路管理及資通安全相關的資訊與技能。

- 工作範圍：
- ① 推廣網路相關應用服務，如網路技術管理維護、網路電話、多媒體影音服務...等
 - ② 辦理主題式研討會，如不當資訊防制、拒絕存取資訊防制機制、網路倫理規範、智慧財產權的宣導、個人資料保護制度之建置經驗分享...等
 - ③ 辦理重點式技術研習會，如 **DNSSEC 建置**、病毒防範技術、資通安全講習、IPv6 作業環境與應用服務建置、IPv6 路由設定與防火牆操作等

四、網路應用特色服務

擴大服務功能、縮減數位落差服務、提供連線單位良好使用介面。

- 工作範圍：
- ① 配合教育部推動縮減城鄉中小學數位落差政策，八年來成效良好，本年度持續推動「縮減數位落差相關服務」工作計畫。預計進行 1~2 次。
 - ② 繼續強化台中區網中心網路氣象台功能，加強使用者介

面功能及應用範圍。提供區網各連線單位能快速、方便了解整個區網中心的網路連線狀況。

- ③ 持續提供 Google Global Cache 服務以因應近年來學術網路多媒體串流(如 YouTube) 流量大幅增加的需求，並有效降低 TAnet 骨幹流量壅塞的情形。
- ④ 持續與中華電信公司合作，提供 CDN 服務，以因應近年來多媒體串流(如 MOD) 流量大幅增加，並有效降低學術網路與 HiNet BGP peering 流量壅塞的情形。**以上兩項服務預計一年約需 10 萬元的維運經費。**
- ⑤ 配合教育部政策，完成教育雲中部資料中心建置及開始提供相關服務。預定目標：(1)預計 104 年第一季完成教育雲中部資料中心建置；(2)協助教育部建立申請教育雲服務之標準程序；(3)協助成立系統移轉輔導團隊；(4)協助教育雲應用服務系統上線；(5)建置 IaaS 雲端管理系統；(6)資源負載平衡與自動擴充；(7)與各教育雲資料中心互相備援；(8)舉辦教育雲資料中心服務推廣說明會。**(本項服務需增聘專任管理人員 1 名，需人事費約 51 萬元)**
- ⑥ 推廣本中心自行開發之「網站應用程式弱點掃描」及「防洩漏個資掃描平台」手持式裝置版本。

五、預期效益

- (一)、針對 TACERT 公佈之『惡意網站威脅來源清單』，除了教育部已在入口進行阻擋的 IP 之外，將利用區網已建置的流量管制設備進行漏網 IP 的阻擋並隨 TACERT 公布之資料更新。此舉應可有效降低不當資訊的流竄，提昇網路使用效率。
- (二)、建立網路使用倫理及尊重智慧財產權的觀念。預計辦理 3~4 場主題式研討會，如網路倫理規範、智慧財產權宣導、個人資料保護、資通安全講習...等。預計有 200 人次參加。
- (三)、提升區、縣市網中心及連線單位網管人員專業素養以及資安防護能力，預計辦理 3~5 場研討會，如不當資訊防制、DNSSEC 建置、拒絕存取資訊防制機制、IPv6 技術...等，預估有 200 人次參加。
- (四)、持續進行中部地區城鄉中、小學數位落差問題改善計畫，並考慮進行跨區網合作。本年度預計進行 1~2 次服務。
- (五)、持續推廣已建置的 SIP Proxy Server 服務，提高連線單位網路電話的使用，以加強彼此間之公務與學術交流，達到縮短反應時間、節約電話費用的目標。預估一年可以有 12,000 筆通話量，節省 20,000 分鐘的通話費用。
- (六)、Google Global Cache 中部營運點，預估可以減少本區網骨幹出口流入量 25~30%。

參、經費需求

- 一、人事費（網管人員 1 名；資安管理人員 1 名；雲端資料中心管理人員 1 名，兼任助理 1 名(半年)）

詳列於附件『104 年度台灣學術網路(TANet)臺中區域網路中心基礎維運與資安人員計畫』中。

- 二、基本營運（教育部補助經常門）

詳見『104 年度台灣學術網路(TANet)臺中區域網路中心基礎維運與資安人員計畫』。