雲嘉區域網路中心

臺灣學術網路(TANet)區域網路中心

107 年度基礎維運與資安人員計畫

106 年 12 月 25 日

【目　　錄】

壹、計畫基本項目 3

貳、計畫執行內容 3

一、區域網路中心基本維運 3

(一)現況說明(含網路架構圖) 3

(二)工作內容 4

(三)辦理資訊推廣活動 6

(四)創新服務 6

二、建構區網中心、連線單位及學校資通安全基本防護環境 8

(一)現況說明 8

(二)區網中心資安防護設施與處理機制 8

(三)資安推廣服務 11

三、區域網路中心特色推動-教育維運雲平台(N-Cloud) 13

(一) N-Cloud 建置說明 13

(二) N-Cloud 建置規劃與服務 13

(三) N-Cloud 建置效益 14

四、106 年度執行成效評量結果改進 15

(一)維運方面 15

(二)資安方面 15

參、經費需求 16

壹、計畫基本項目

一、計畫期程： 107 年 1 月 1 日 至 107 年 12 月 31 日

二、計畫執行單位： 國立中正大學

貳、計畫執行內容

一、區域網路中心基本維運

(一)現況說明(含網路架構圖)

雲嘉區域網路中心自民國 80 年 4 月成立以來，服務雲嘉區域各級學校及單位，即將邁入第 27 個年頭了。

現階段提供 40 Gigabit 的電路介接於台灣學術網路(TANet)骨幹上，目前直接介接於本中心計有 32 個單位，依性質分別為 22 個學術單位、3 個研究單位及 7 個 ISP 業者。這些單位包括縣市教育網路中心 3 個單位、專科以上學校有 11 所、高中職學校有 8 所及 3 個研究單位。另外 TWAREN 研究網路也提供 20G 頻寬與 TANet 骨幹銜接，並提供區域內各單位連接使用，目前有嘉義大學等 8 校連接。

雲嘉區網轄區有三個教網中心分別為嘉義縣教育網路中心、嘉義市教育網路中心及雲林縣教育網路中心，三單位由中華電信及亞太電信各提供 4G 頻寬介接於雲嘉區網中心，特別是嘉義市教育網路中心，在 91 年 12 月 9 日將所屬連線學校頻寬全部提昇至 Gigabit，成為 TANet 第一個擁有 Gigabit 頻寬的教育網路中心。

為了讓區域內單位網路互連順暢及資訊安全基礎防護，區網中心提供各種網路路由器及網路資安相關設備，說明如下：

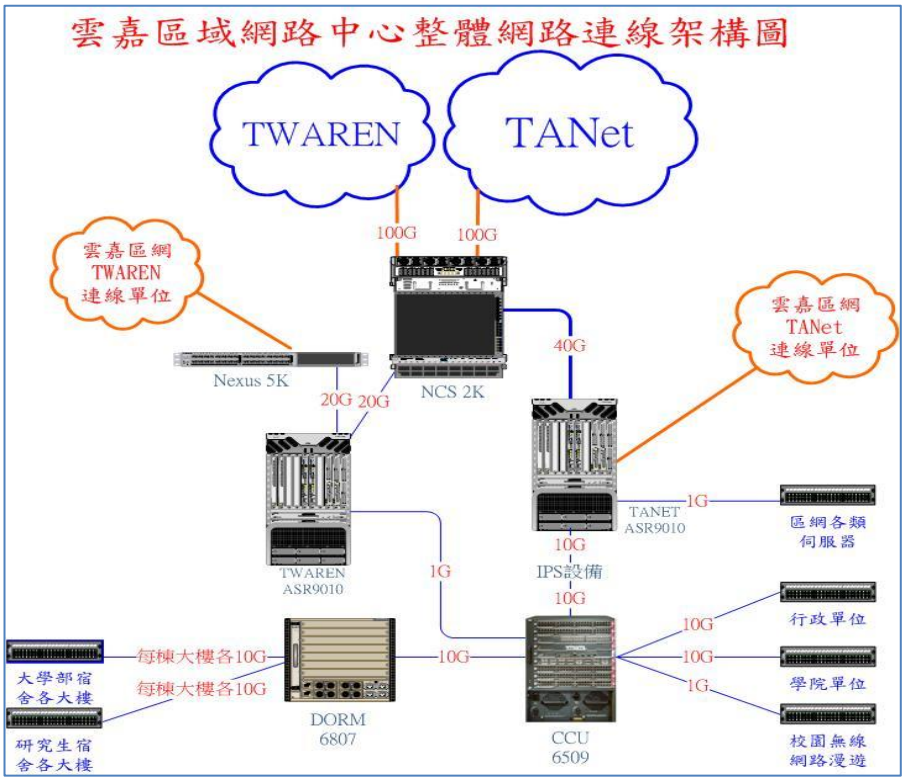
（1）路由設備：Cisco ASR9010 二部、Cisco 6807 二部、Cisco 6509 Router 二部。

（2）網路相關設備：Cisco 2916 Switch 一部、Cisco 2950 Switch 八部、Cisco Catalyst 2900 Hub 二部、Foundry Server Iron 三部、Wave Switch 1216 Hub 二部、iTaiwan 無線上網服務及校際漫遊 Access Point (AP) 約 135 部。

（3）資訊安全設備：網路威脅管理與防禦系統 TippingPoint 2500N、SMS 管理伺服器一部，8e6 不當資訊防治系統一部、8e6 報表產生器一部、

網站應用程式弱點監測系統二部、教育機構防洩漏個資掃瞄系統一部、應用程式防火牆(WAF)一部、SSL VPN 一部。

（4）各類伺服器設備：雲嘉區網提供各類電腦主機伺服器數拾部，包括 Web Server 二部、E-mail Server 十部、Proxy Server 八部、DNS Server 七部、FTP Server 二部、Roaming Server 一部、Radius Server 一部 、無線網路伺服器 Wireless Gateway(Cisco Control Module)一套及 Cisco WiSM-2 server 一部、Cisco WLC server 一部、Nopam Server 拾餘部、不當資訊防治系統主機一部及流量統計監測主機(Netflow Server) 二部等資訊服務系統供校內外師生使用。



(二)工作內容

為推動本年度雲嘉區域網路中心各項基本業務、重點任務及委辦任務，本中心擬辦各項工作內容如下：聘用一位網管人員專屬處理區網網路管理及一般行政業務，另聘用一位資安人員專屬處理區網資通安全相關業務、巡迴連線單位舉辦各種研討會、定期召開雲嘉區域網路管理委員會、協助本區域縣市教育網路中心網路管理、技術諮詢服務及專業教育訓練、提供各種資訊服務系統（包括 BBS、FTP、NEWS、PROXY、MAIL RELAY、DNS、Netflow 流量統計、Nopam 無痛式垃圾郵件過濾系統、Wireless 校際漫遊等），負責雲嘉區域網路運作管理以確保網路暢通、技術支援雲嘉區域各級學校、資通安全宣導與推廣、網路資源及管理資訊透明化、IP/DNS

管理核發、IPv6 推廣、VoIP 網路電話推廣、SIP/ENUM 推廣與宣導、RFID 運用推廣、SPAM 問題的處理、侵權問題的處理、區域內流量統計與監測、提供無線網路校際漫遊機制服務、智慧財產權之宣導、法律規章之宣導、協助推廣 NuWeb 之使用並建立校園網路社群等，以及執行鈞部委辦各種業務。

重點任務方面：包括加強網路及資訊安全管理、網路侵權處理、加強電腦病毒防治、加強不當資訊防治、推動區域內各單位資通安全演練及防範機制，加強連線單位各項服務，強化校際無線網路漫遊環境及各項創新服務推廣等。

諮詢服務方面：為了提昇對雲嘉區域各級學校師生之服務品質，本中心每年均聘請數位有電腦相關知識之工讀生提供諮詢服務，每天安排諮詢工讀生值班，提供諮詢服務，以解答各種電腦問題，並排解印表機及使用上的問題，成效良好；其次本中心管理之 CNA(Campus Network Association)社團負責協助中心管理校內及宿舍網路，並提供諮詢及網路維修服務。

各級連線學校互動方面：平時透過電話或 E-mail 互相交流，每學年定期召開雲嘉區域網路管理委員會二至四次，提供各級連線學校互相交換意見，以達區域和諧，並於會議上提供技術研討，以提昇電腦暨網路相關知識，並促進雲嘉區域各級學校電腦及網路之技術水準，進而提昇使用及管理能力。

研討會方面：本中心為了提昇雲嘉區域各級學校師生對電腦及網路的使用及認識，本中心資訊推廣組每學期安排一系列的教育訓練課程供雲嘉地區師生自由參加，中心也舉辦定期與不定期各種研討會，以提昇本區師生對電腦及網路相關知識，尤其協助對本區域資訊教師的專業訓練，期望能讓這些種子教師能把技能帶回學校教導該校師生，進而達成全區師生皆會使用電腦及網路為目標。

資訊系統服務方面：本中心提供各種服務系統包括 PROXY、MAIL RELAY、DNS、WWW、Nopam、NuWeb、NuBlog、NuCloud 等，以滿足全區師生對各種資訊的需求，能力所及也協助縣市教育網路中心建置各種服務系統。

確保區域網路暢通方面：隨時透過中心建立各種網路管理系統監測，以了解連線學校網路是否暢通，如遇線路故障，立即通知相關單位及所屬 ISP 業者，請其即刻處理，以確保網路暢通，維護使用者權益。

機房監控與管理方面：本中心針對機房之安全區域設有 IC 感應設備，進行門禁之管制，未具機房權限者將無法進出，另有監視系統、環控系統及空調系統等，即時對機房之狀況進行側錄及溫濕度之控管，並對不正常之運作狀況以簡訊、E-Mail 通報管理人員掌握狀況，以確保雲嘉區網之網路、系統持續提供服務及正常維運。

流量統計方面：中心建有流量統計監督系統，每天對連線單位做流量統計(含 IPv6)，並對校內宿舍做網路傳輸量前 100 名排名，並管制每天每人流量 5G，超過管制量者系統自動給予斷線處理。另對雲嘉地區所有使用者做網路傳輸量前 100 名排名，遇有異常使用時，立即通知該單位改善，不改善者，必要時給予該 IP 斷線處理，等其處理後，始給予恢復網路暢通，自實施以來成效非常良好，已大幅改善不當使用情形。

(三)辦理資訊推廣活動

網路使用所造成的種種問題，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。

區網中心 107 度將以下列方式辦理資訊推廣活動

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、 DDoS 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，如封包分析、惡意程式或病毒防範技術、資通安全講習、IPv6 作業環境與應用服務建置及操作等。

(四)創新服務

在創新服務方面，在本校所有同仁不遺餘力的努力下，都有不錯的成果，分別簡述如下：

1.Nopam 無痛式垃圾郵件過濾系統：

本計畫由本中心主任李新林教授擔任計畫總召集人，本校網際網路研究中心主任資工系吳昇副教授任技術召集人及若干研究生等人參與，並共同開發系統，以雲嘉區網提供測試環境，部分中心同仁協助測試系統成效，經實際測試，此一 Nopam 垃圾郵件過濾系統不僅有高達 97-98%之偵測率、

低至萬分之一之誤殺率，且具有高速的效能，在一般 Intel P4 機器，一天可以處理超過一百萬封信件，成效卓越。自 94/8/12 首次發表以來，為了提供更好的服務，我們一直在努力繼續開發系統，並已經更新過數個系統版本(最新版本 Nopam 無痛式垃圾郵件過濾系統 2.3 版於 96/3/16 發行)，團隊成員的努力，有目共睹，我們也期待能提高更好的效能。本系統已於 94/10/15 免費提供教育學術單位下載使用，迄今已有全國 80 餘個學校單位在使用。

網址：http://nopam.ccu.edu.tw

2.辦理大學甄選入學彙辦業務

本校於 92~106 年度連續十餘年辦理大學甄選入學彙辦業務，深受各界好評，大學招生委員會聯合會決定繼續委以重任，請本校續辦「107 年度大學甄選入學彙辦」業務，本校所有參與業務的同仁也義不容辭的接下此艱鉅的業務，各項業務目前正在進行中。

網址 ：https://www.caac.ccu.edu.tw/

3.NUCloud 雲端推廣

本校開發之 NUCloud 雲端技術，以個人網站及部落格方式呈現，提供同學完整在校的學習歷程檔案、免費雲端空間、個人知識管理平台、協同合作及上傳個人創意作品之展示平台，展現學生在就學期間的創作或創意，藉由實體、虛擬的，讓他校師生，甚至是業界得以看到本校學生的才幹，藉由創意的交流，增進跨領域學習、溝通能力，引介合作，提升跨領域創作能量。

網址：http://cloud.ccu.edu.tw

4.資訊能力測驗系統推廣

本系統由本校自行開發，自 91 年度開始提供學生資訊能力檢測，本校大學部同學需經本系統檢測及格使能畢業，另並以循序漸進方式新增檢定科目，以符合各學院專業技能需求，增進學生畢業後之競爭力；現階段我們也努力推廣其他學校使用，目前我們已輔導 3 所大專院校使用本系統。
網址 ：http://infotest.ccu.edu.tw/

5.辦理 107 年度大學甄選入學線上書審業務

係因大學甄選入學委員會執行「大學甄選入學之個人申請招生管道推行書面審查電子化計畫」，其宗旨為減輕考生負擔，簡化大學行政流程與縮短資料傳遞時間，同時減少紙張用量等。102 年 24 所大學試辦成效良好，103 年以後將全面辦理。

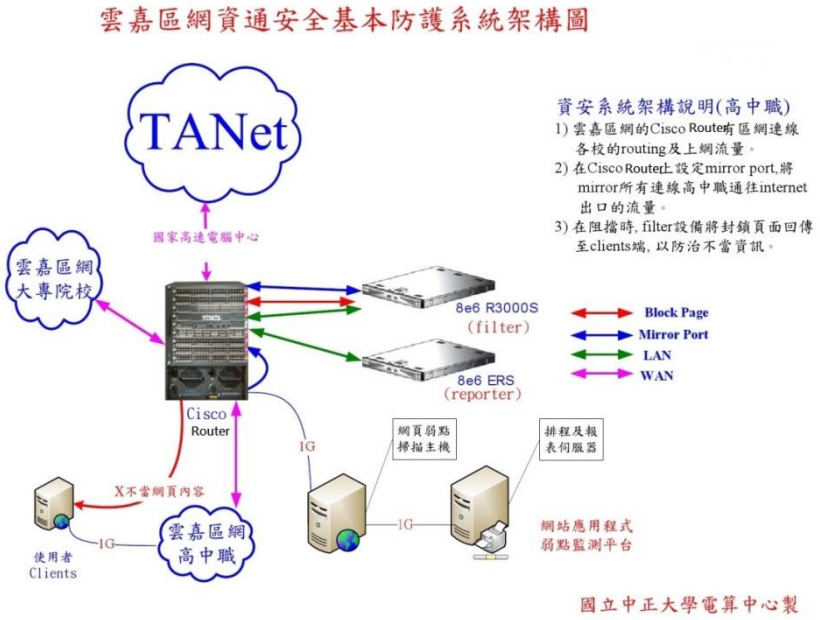
網址 ：https://www.caac.ccu.edu.tw/

二、建構區網中心、連線單位及學校資通安全基本防護環境

(一)現況說明

隨現代資訊化社會的來臨，政府部門積極推動我國資通安全基礎建設，協助政府機關及重要民間業者之資通訊及網路系統，當遭受外來因素破壞或不當使用等緊急事故發生時，能迅速通報及緊急應變處置，以降低該事故可能帶來之損害。教育部亦要求所屬學校單位，透過有效的資訊安全管理，來防止重要資訊受到潛在威脅的破壞，進而全面提升校園資通安全防護水準。

區網中心運用相關資安系統，於 TANet 網路連外出入口，阻擋非法連線，提昇網路服務品質，強化連線學校網路資安實體環境防護機制。

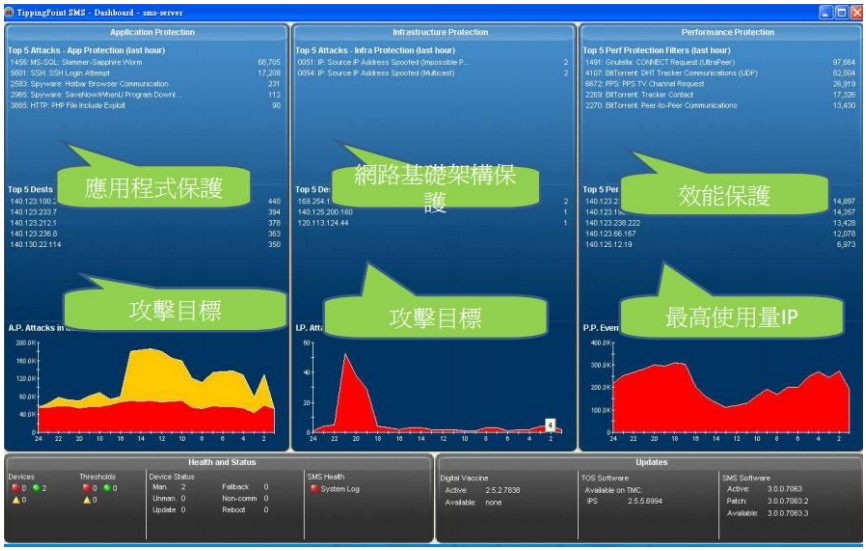


(二)區網中心資安防護設施與處理機制

1. 網路威脅管理與防禦系統 TippingPoint (IPS)

- 運用 IPS 網路威脅管理與防禦伺服器，防止已知和未知的網路威

脅，監控和阻止惡意網路活動，降低 TANet 網路頻寬，提昇網路頻寬流量，有效阻擋絕大部分病毒攻擊或駭客入侵動作。



2. 網站應用程式弱點監測系統

- 配合教育部「教育單位網站應用程式弱點監測平台」計畫，所建置之弱點掃描系統，協助連線之高中職以上學校，進行網頁弱點之掃描，降低網站被入侵之風險。網址為 http://ewavs.ccu.edu.tw。

3. 教育機構資安通報平台

- 為求有效掌握所屬之各連線單位之資通訊及網路系統現況，避免各單位之系統遭受破壞與不當使用，預期能迅速通報及緊急應變處理，並在最短時間內回復，以確保各級教育機構之正常運作。

網址為 https://info.cert.tanet.edu.tw/prog/index.php

4. 流量管理及監測系統 Service Control Engine (SCE)

- 面對現今不斷成長、愈趨複雜的網路環境，目前應用流量管理及監測系統 Service Control Engine (SCE8000)一部，迅速且準確分類出各類網路流量，產生最適切有效的統計分析數據，隨時監控網路的運作狀態。

5. 教育機構防洩漏個資掃瞄平台

- 提升台灣學術網路資通安全防護與建立友善上網環境，針對單位網站進行有無個資訊息不當揭露的問題，進行網頁內個資之掃描，以降低個資外洩風險。http://wwwsec.ccu.edu.tw。

(三)資安推廣服務

107 年度區網中心資通安全業務將要推動之事務說明如下：

1、在協助連線學校資訊安全管理制度(ISMS)業務推動方面

提供區網中心在導入 ISMS 管理制度歷程中之經驗，中心目前有七位同仁通過「資訊安全管理系統主導稽核員訓練課程」(ISO27001 Lead Auditor Training Course Certificate)並取得證書，以上人員將協助相關業務。另備有諮詢專線，讓連線學校在導入過程中有任何疑問都可透過專線隨時洽詢，同時協助 ISMS 管理制度內部稽核作業。

2、建立網路安全防範機制方面

運用區網中心入侵偵測系統(IPS)，於 TANet 網路連外出入口，阻擋非法連線，提昇網路服務品質，強化連線學校網路資安實體環境防護機制。在資安預警情資方面，當資訊設備疑似具有資安漏洞、成為駭客攻擊跳板、連線駭客中繼站、存在惡意程式、敏感資訊疑似遭洩漏等可疑的資安行為時，協助第一線單位進行處理，避免事件繼續擴大，造成更大損失。

3、建立符合行政院資通安全規定之網路安全通報機制

區網中心持續配合 TACERT 組成資訊安全技術服務團隊，執行資安相關資通安全通報應變作業，當各單位及系統遭受破壞與不當使用時，透過通報及緊急應變處理機制在最短時間內回復，以確保各級教育機構之正常運作。

4、研討會及相關教育訓練辦理

本區網中心 107 年度將舉辦至少 2 場次資安研討會(資安技術、認知教育訓練及宣導活動)及各一場次智慧財產權、個資法研討會，除強化各校教師或網管人員對資通安全之認知，同時強化各連線學校師生智慧財產權及資法之認知，並建議參與研習人員回校後能有效推動相關之宣導。

5、網站應用程式弱點監測及個資掃瞄之執行

配合「教育機構防洩漏個資掃瞄平台」計畫，提供 TANet 連線單位申請網站個資掃瞄服務，協助各教育單位避免其網站之開放區域有洩漏個人資料的情事，以自動化方式掃瞄申請單位轄下之網站，分析其個資洩漏的狀態與風險，提升 TANet 個資防護水準。同時延續「教育單位網站應用程式弱點監測平台」計畫，協助區網中心高中、職以上連線學校進行網站弱點（包含 SQL Injection 、XSS）掃描、健檢，以及資安演練等相關服務。

6、BCP 營運持續演練

持續推動網路中心營運持續演練，以供中心人員在危害系統事件發生時，採取正確的應變措施，以降低對中心正常運作的威脅所造成之衝擊，提昇資訊安全服務品質。

7、智財權檢舉案件追蹤

除持續智慧財產權宣導，以強化保護智慧財產權之觀念，期使師生對於智慧財產權的認知能更加確實。同時將針對所發生之智財權檢舉案件持續追蹤。

8、連線學校端採購的網路設備可以將產生的日誌交給N-Cloud

各校的網管老師能夠把學校內的網路設備日誌與流量(NetFlow/sFlow)上傳到建置於區網中心的N-Cloud，N-Cloud是連線單位共用的網管中心(NOC)也是資安中心(SOC)，針對各校內部的網路與資安狀態進行持續性監控與分析工作，並提供各種簡單明瞭的報表直指網路障礙根源。

三、區域網路中心特色推動-教育維運雲平台(N-Cloud)

(一) N-Cloud 建置說明

當今資安威脅日益嚴峻，顯現在校園網路裡最常見也是最困擾的狀況，就是校內電腦中毒成為 Botnet 後所帶來一連串的網路障礙，影響教學。新一代的校園網路維運觀念著重與流量分析與資安技術的整合，快速定位並移除障礙根源，確保校園網路永保安康。

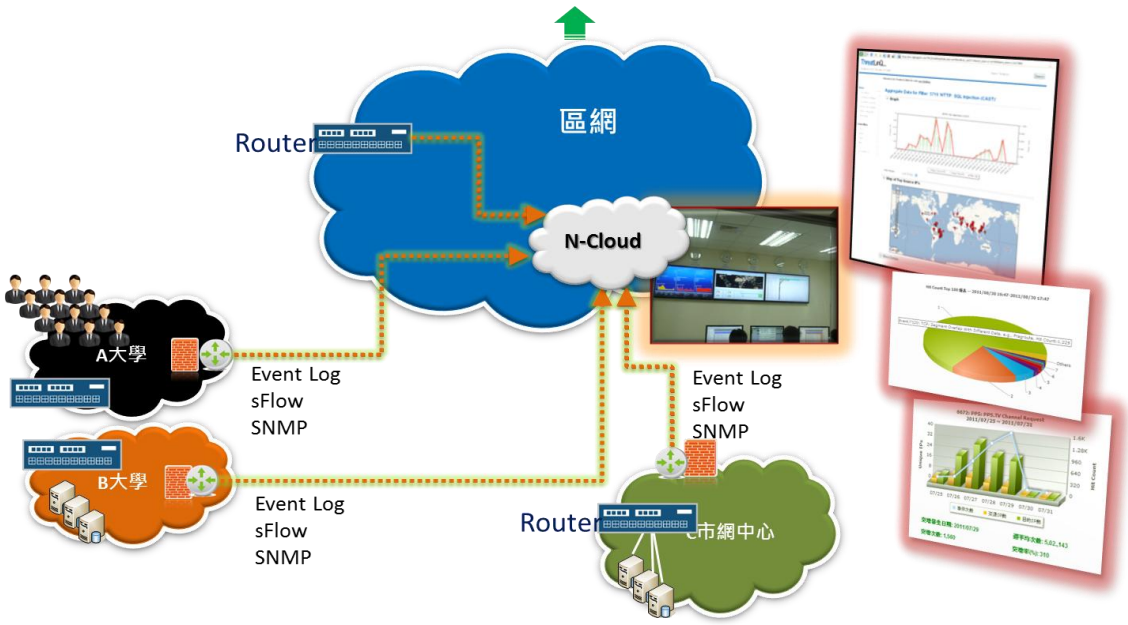
然而，對於許多負責學校網路管理的老師來說，不僅無法申請足夠的經費採購資安防護設備或是佈署網管工具，往往也沒有與專職的時間能夠做到上述的快速排除障礙。

(二) N-Cloud 建置規劃與服務

區網中心初期規劃，希望運用雲計算技術監控並分析學校的網路健康狀態與資安事件，在網路障礙發生的當下就能夠知道原因並定位導致問題的來源所在位置，協助網管老師在最短時間內排除障礙恢復校園網路的最佳連線品質。

區網將建構即時且自動化之網路品質監控系統

-佈署教育維運雲平台(N-Cloud)



-High Level 觀點,隨時掌握各校狀態

(三) N-Cloud 建置效益

- 讓蒐集與分析全域的建置成本大幅降低
- 全面提升各校的網路與資安技術能力
- 讓中心端資安與網路設備的訊息傳達更有效益
- 讓網路維運變得容易，除錯時間大幅縮短

四、106 年度執行成效評量結果改進

(一)維運方面

1. 提供區域網路中心 RWD 響應式網站服務，並提升更好的網站內容服務及績效呈現，讓連線單位獲得最佳資源提供。
2. 強化推廣連線單位支援 IPv6 之連線能力，並支援技術能力較弱之單位建置 IPv6 之應用服務。
3. 針對區域網路中心連線單位進行最適宜之訓練課程規劃，並將課程內容以數位影音方式留存，讓資訊分享發揮更大效益。

(二)資安方面

1. 加強宣導教育機構資安通報平台規定之通報機制，參考及引進其它區網(如中興區網)作法，以降低資安服務之通報及應變處理平均時數。
2. 引進中央桃園區網 spark 異常流量監測系統，提供連線單位使用，以強化區域網路中心資訊安全警示。

參、經費需求

一、人事費（網管人員 1 位；資安人員 1 位）

1.為了推動雲嘉區網各項營運業務需要，擬續聘網管人員一位，負責管理區網中心各種網路設備、伺服器及辦理行政業務。

2.資通安全基本防護工作之推動，擬續聘資安管理人員一位，以處理區域內各類資安問題及協助連線單位資安相關業務之推動。

二、基本營運（教育部補助經常門）

雲嘉區網基本營運之各項業務推動，所需費用如附檔「臺灣學術網路區域網路中心 107 年度基礎維運與資安人員計畫經費申請表」所列。

三、發展區域特色（教育部補助經常門）

教育維運雲平台(N-Cloud)建置及創新服務經費需求：由區網經費編列建置設備、維護及服務人力等費用，初期約需 20 萬元整。