

107 年度區域網路中心年終成果基礎資料彙整表

桃園區域網路中心

(負責學校：國立中央大學)

107 年 11 月 22 日

目錄

壹、 基礎維運資料.....	1
一、 經費及人力.....	1
二、 基礎資料(網管及資安).....	2
三、 請詳述本部補助貴區網中心網管及資安人力之服務績效.....	4
貳、 請詳述貴區網中心之網路連線、網管策略及具體辦理事項(網路管理).....	5
參、 請詳述貴區網中心之資安服務、資安政策及具體辦理事項(資安服務).....	6
肆、 請說明貴區網中心服務推動特色、辦理成效與未來營運計劃(特色服務)..	7
伍、 前(各)年度執行成效評量改進意見項目成效精進情形.....	9
附表 1：區網網路架構圖.....	10
一、 區網與連線單位(含縣(市)教育網路、連線學校、其他連線單位等)、TANet、Internet(Peering)的總體架構圖.....	10
二、 網路配合各種應用架構(如連線分流、頻寬管理)或資安架構(防火牆、IDS/IPS/WAF)的規劃或實際運作架構.....	11
附表 2：連線資訊詳細表.....	12

壹、基礎維運資料

一、經費及人力

請依下列項目提供本年度報告資料

1. 網路中心經費使用	(1) 核定計畫金額： <u>4,690,000</u> (2) 教育部補助金額： <u>3,430,000</u> (3) 自籌金額： <u>1,260,000</u> (4) 實際累計執行數（至 11 月）： <u>77%</u>
2. 網路中心人力數	(1). 專任： <u>3</u> 人 (2). 兼任： <u>4</u> 人（請填數字）。 其中包含教育部補助： (1). 網管人員： <u>2</u> 人，證照數： <u>2</u> 張。 (2). 資安人員： <u>1</u> 人，證照數： <u>1</u> 張。

二、基礎資料(網管及資安)

請依下列項目提供本年度報告資料

(一)區網中心連線資訊彙整表

	項目	縣(市)教育網中心	大專校院	高中職校	其他學校	其他單位	總計	
(1) 連線數 (以單位(校)數統計)	單位(校)數	3	14	18		8	43	
	連線比例						註：單位(校)數 / 總計	
(2) 連線頻寬 (以電路數統計)	專線							
	光纖	10M(不含)以下						
		10M(含)以上 100M(不含)以下			4		4	
		100M(含)以上 1G(不含)以下		5	14		8	27
		1G(含)以上 10G(不含)以下		9				9
		10G(含)以上						
		其他(如 ADSL 等)						
	連線電路小計							
(3) 連線縣(市)教育網路中心	縣(市)教育網路中心		連線頻寬(1)		連線頻寬(2)		備註	
	1.	桃園市網	10G(亞太電信)		2G(中華電信)		ipv4-10G ipv6-2G	
	2.	連江縣網	1G					
	3.	金門縣網	1G					
(4) 連線其他單位 (非 ISP)	其他單位名稱		連線頻寬(1)		連線頻寬(2)		備註	
	1.							
	2.							
	3.							
	4.							
	5.							
(5) 連線 TANet 及其他 ISP 線路	臺灣學術網路(TANet)		連線台北主節點		連線新竹主節點			
			頻寬 <u>100</u> Gbps		頻寬 <u>100</u> Gbps			
	其他 ISP		連線頻寬(1)		連線頻寬(2)		備註	

	1.	HINET	2G		
	2.	SeedNet	1G		
	3.	亞太線上	100M		
	4.	和信	1G		
	5.	速博	1G		
	6.	台固	1G		
(6) 補充說明：					
(7) 連線資訊	請依附表「學校/單位連線資訊詳細表」格式填附				

(二) 區網中心資訊安全環境整備表

<p>(1) 網路中心及連線學校資安事件緊急通報處理之效率及通報率。 (由教育部資科司提供數據)</p>	<p>1. <u>1、2 級資安事件處理：</u> (1) 通報平均時數：<u>3.924</u> 小時。 (2) 應變處理平均時數：<u>0.024</u> 小時。 (3) 事件處理平均時數：<u>3.949</u> 小時。 (4) 通報完成率：<u>95.15%</u>。 (5) 事件完成率：<u>99.2%</u>。 2. <u>3、4 級資安事件通報：</u> (1) 通報平均時數：<u>無</u>。 (2) 應變處理平均時數：<u>無</u>。 (3) 事件處理平均時數：<u>無</u>。 (4) 通報完成率：<u>無</u>。 (5) 事件完成率：<u>無</u>。 資安事件通報審核平均時數：<u>2.035</u> 小時。</p>
<p>(2) 網路中心配合本部資安政策。</p>	<p>1. 資通安全通報應變平台之所屬學校及單位的聯絡相關資訊完整度：<u>97.06</u> %。 (由教育部參照資安通報演練作業現況提供) 2. 區網網路中心依資通安全應執行事項： (1) 是否符合防護縱深要求？ <input checked="" type="checkbox"/>是 <input type="checkbox"/>否 (2) 是否符合稽核要求？ <input checked="" type="checkbox"/>是 <input type="checkbox"/>否 (3) 符合資安專業證照人數：<u>22</u> 員 (4) 維護之主要網站進行安全弱點檢測比率：<u>100</u> %。</p>

三、請詳述本部補助貴區網中心網管及資安人力之服務績效

1. 網管人力：

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 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。

2. 資安人力：

資安通報審核及演練，資安事件處理，社交演練，異常流量 ip 偵測及處理，協助 ISO27001 資安認證，弱點掃描及追蹤處理，個資保護系統維護，辦理資安研討會，臨時交辦事項。

貳、請詳述貴區網中心之網路連線、網管策略及具體辦理事項(網路管理)

1. 區網對外透過 source fire IPS 進行異常網路行為的入侵防禦。
2. 今年重新開發建置桃園區網中心新網站 <http://web.tyrc.edu.tw>，以使用者為中心提供更友善服務。
2. 即時流量監控，掌控流量變化
<http://cacti.tyrc.edu.tw/tyrc.html>。
3. 計算流量 Top N 系統，監控大流量 ip
<http://hadoop.tyc.edu.tw>（讀取權限的帳號/密碼： tyrc /tanet_tyrc）。
4. 建置 GGC 加速 google 網站的服務。
5. 協助連線單位啟動 ipv6 連線 <http://web.tyrc.edu.tw:8080/IPV6>
及監控 ipv6 mrtg 流量變化

其餘請參見年終執行成效評量簡報檔

參、請詳述貴區網中心之資安服務、資安政策及具體辦理事項(資安服務)

1. 桃園區網中心已連續十年取得 ISO27001 認證,今年 3 月並依規定接受 ISO 27001 改版複查以保持證照有效性,提供本大學資訊技術及台灣學術網路桃園區域網路中心相關之服務。
2. 啟動 Cisco Source Fire IPS inline 功能,制定 policy 進行 Vulnerability Protection, Anti spyware ,URL filtering 保護有效降低網路攻擊事件。
3. 建置 Spark 異常流量偵測系統,偵測異常流量,即時解決網路異常。
<http://hadoop.tyc.edu.tw> (讀取權限的帳號/密碼: tyrc /tanet_tyrc)
4. 加入北區學術網路 SOC(台大)計畫,提供資安防護與資訊分享機制,監控網路異常 ip。
5. 辦理資安及網路管理教育訓練及研討會。
<http://web.tyrc.edu.tw:8080/teach>
6. 新版教育體系資通安全暨個人資料管理規範上路,中央大學以學務處為代表,105 年 12 月率先通過驗證,成為國內首批通過教育體系個人資料管理規範驗證學校之一。目前全校共有 22 個一級單位擔任推動窗口,並已完成 72 個一、二級單位導入 BS 10012 個人資料管理系統 (PIMS)。
<http://www.ncu.edu.tw/campus/article/1968> 、<https://pims.ncu.edu.tw/codes/index-1.php>

其餘請參見年終執行成效評量簡報檔

肆、請說明貴區網中心服務推動特色、辦理成效與未來營運計劃(特色服務)

1. 服務推動特色、辦理成效。

1.1 Open Source SIEM 系統之導入與應用

桃園區網中心透過導入 Open Source SIEM (Security Information and Event Management) 系統，即時監控網路行為，並且針對主機入侵偵測系統 Host-Based Intrusion Detection System (HIDS)、網路入侵偵測系統 Network Intrusion Detection System (NIDS) 及入侵防禦系統 Intrusion Prevention System (IPS) 等系統事件收集、管理及分析，並藉由 SIEM 系統的視覺化儀表板、警示訊息、報表等功能，提供關連的資安事件，因此可減輕網路管理人員的工作負荷。相關導入經驗撰寫論文投稿至 TANET2018 研討會，獲得佳作論文獎。

1.2 雲端 Spark 異常流量偵測系統

以處理巨量資料速度更快的 Spark 架構結合原 FDNS 系統之 Hadoop 架構，彌補 Hadoop MapReduce 的緩慢，系統可於監測大量的網路流量中篩選出異常的流量及可疑主機，並將資料寫入 Mongo 資料庫，提供網管工作人員透過 web 介面查詢每十分鐘、每小時、每天之異常之網路流量及可疑主機排行。系統並已推廣至花蓮區網及高屏澎區網使用，本年度並增加對 IPv6 的支援。

系統優點如下

- (1) 使用 Spark 協同 Hadoop 架構偵測網路異常流量的平台。
- (2) Spark 模組負責即時的運算，可以充分利用 Spark in-memory computing 特性，在大量的 NetFlow Data 中快速篩選出異常網路行為的主機。Hadoop 模組則處理大量批次作業，以每小時進行大量資料分析作業。

1.3 承辦 TANET2018 研討會

TANET 臺灣網際網路研討會係由教育部與臺灣學術網路各區域網路中心於 1995 年共同創辦，第一屆在國立中央大學開始舉辦，時隔至今已 24 載再次由中央大學承辦第二十四屆臺灣網際網路研討會(TANET 2018)。本屆研討會與科技部資訊工程學門、智慧計算學門共同辦理成果發表會，並與桃園市政府資訊科技局同場舉行 OpenData X AR/VR 黑客松競賽決賽。

今年論文的徵稿主題包含 5G 與 IOT、網際網路、行動及雲霧運算、資訊安全、人工智慧、智慧生活、智慧校園、數位金融、互動多媒體 與資訊應用、資訊軟體、智慧學習及其他相關議題，共計 12 大主題、51 個領域。論文收錄篇數接近 500 篇為歷屆 TANET 研討會之最，更首創先例開辦 Birds of a Feather(BOF)議程，提供第一線教學現場老師及網路管理實務人員之交流園地。本屆大會所規劃鼓勵論文投稿者相當豐富的獎勵措施，設立頒發的獎項有傑出論文獎、最佳論文獎、佳作論文獎、最佳口頭發表獎及最佳海報展示獎等，得獎者除獲得書面證書外，更將獲得區塊鏈型態的證書，可在區塊鏈中公開查詢及驗證得獎內容，此亦為本屆 TANET 首創、更是全球第一個頒發區塊鏈得獎論文的研討會。

1.4 教育雲北區雲端資料中心：

提供的資源：

CPU: 216 vCPU (108 core) , RAM: 1136 GB , HD: 可用 70TB (鏡像的備份)

使用的軟體：

雲端管理軟體:VMware (2016/4/28 完成轉換)

虛擬化儲存軟體: (共契採購)

教育雲上的服務系統：

數學小學堂系統 (3 vm)

中華開放教育平台 (11 vm)

體育雲-全民運動資訊系統 (13 vm)

體育雲-全民運動資訊系統報名網站(9 vm)

體育資訊雲端 (3 vm)

教師研習平台 (2 vm)

臺灣微積分題庫 (1 vm)

教育體系單一帳號驗證授權平臺(10vm)

開放教育資源系統 (1 vm)

英語線上學習平台 (2 vm)

教育單位弱點檢測平台 (1 vm)

2. 未來運營計劃(特色服務)。

- 2.1 辦理連線單位建議的教育訓練及研討會：網路管理、物聯網或 AI 相關概念與應用、資安、網路智財權、資安鑑識、雲端運算。
- 2.2 區網主幹轉送封包之監聽/分析/攻擊偵測，Spark 異常流量偵測系統更新及特色推動。
- 2.3 持續辦理離島研討會。
- 2.4 加強雲端服務:提供建置私有雲及教育雲服務之經驗分享/推廣。
- 2.5 協助連線學校 IPv6 建置與推廣。

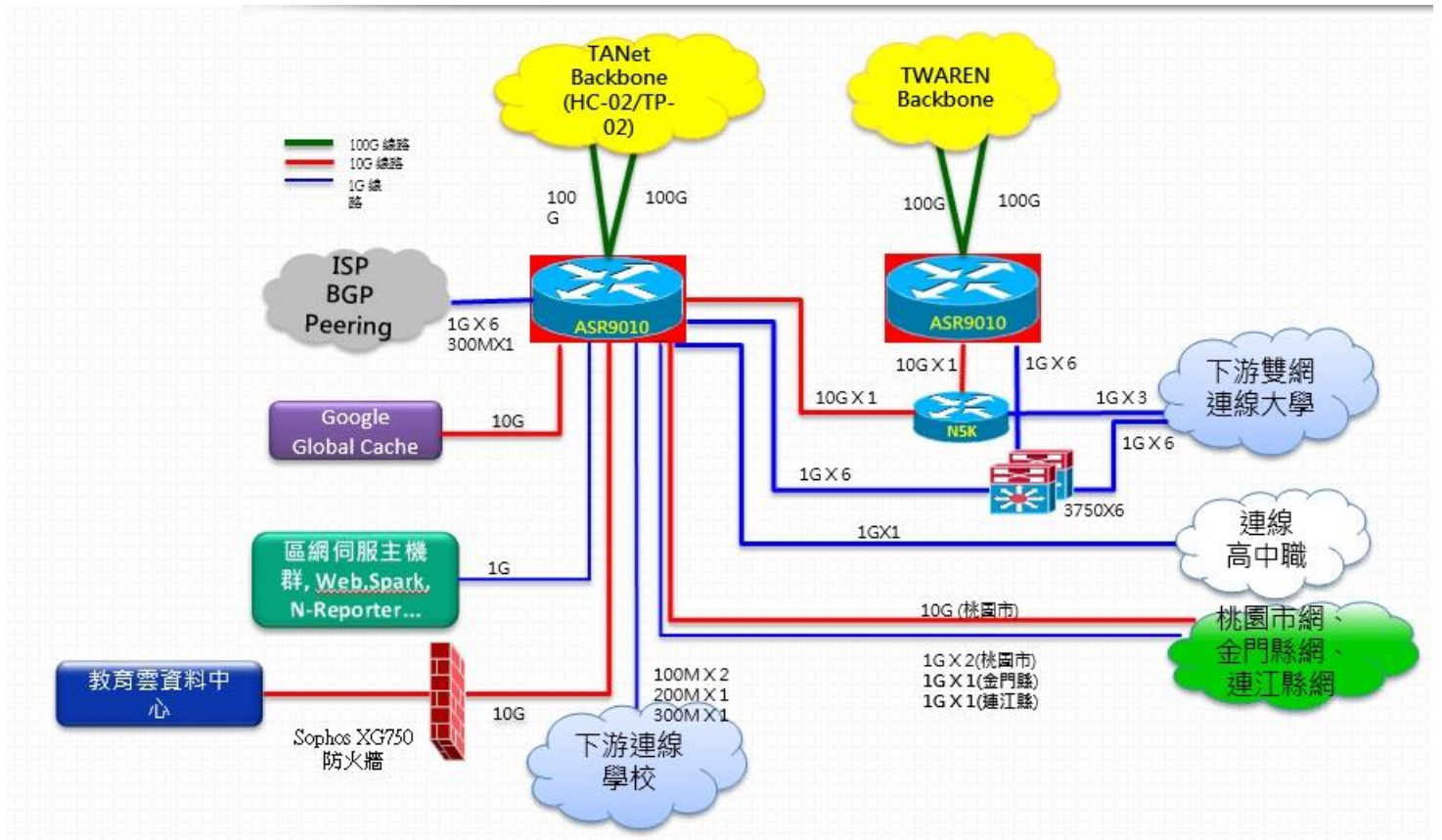
伍、前(各)年度執行成效評量改進意見項目成效精進情形

1. 啟用桃園區域網路中心新網站 web.tyrc.edu.tw，以使用者為中心提供更友善服務，並將維運人力及聯絡方式呈現在區網網站，方便溝通及聯繫，原 www.tyrc.edu.tw 逐步退出服務行列。
2. 資安事件處理除透過自動轉通告系統即時通報連線學校，二小時未填單將以電話再度通知聯繫處理情形，並持續關懷處理時效較長的連線學校。
3. 原定今年於金門縣網辦理離島的研討會，因本年度承辦 TANET2018 台灣網際網路研討會，人力不足，今年暫緩實施，日後將持續每年的離島的研討會，以加強和縣市網之間的交流與溝通。
4. 各類服務網站已調整為使用網域名稱，而非僅使用 IPV4 位址作為 URL 並支援 IPV6。
5. 持續於區網管審會議及教育訓練推動 IPV6，並於區網網頁顯示整體 IPV6 概況。

附表 1：區網網路架構圖

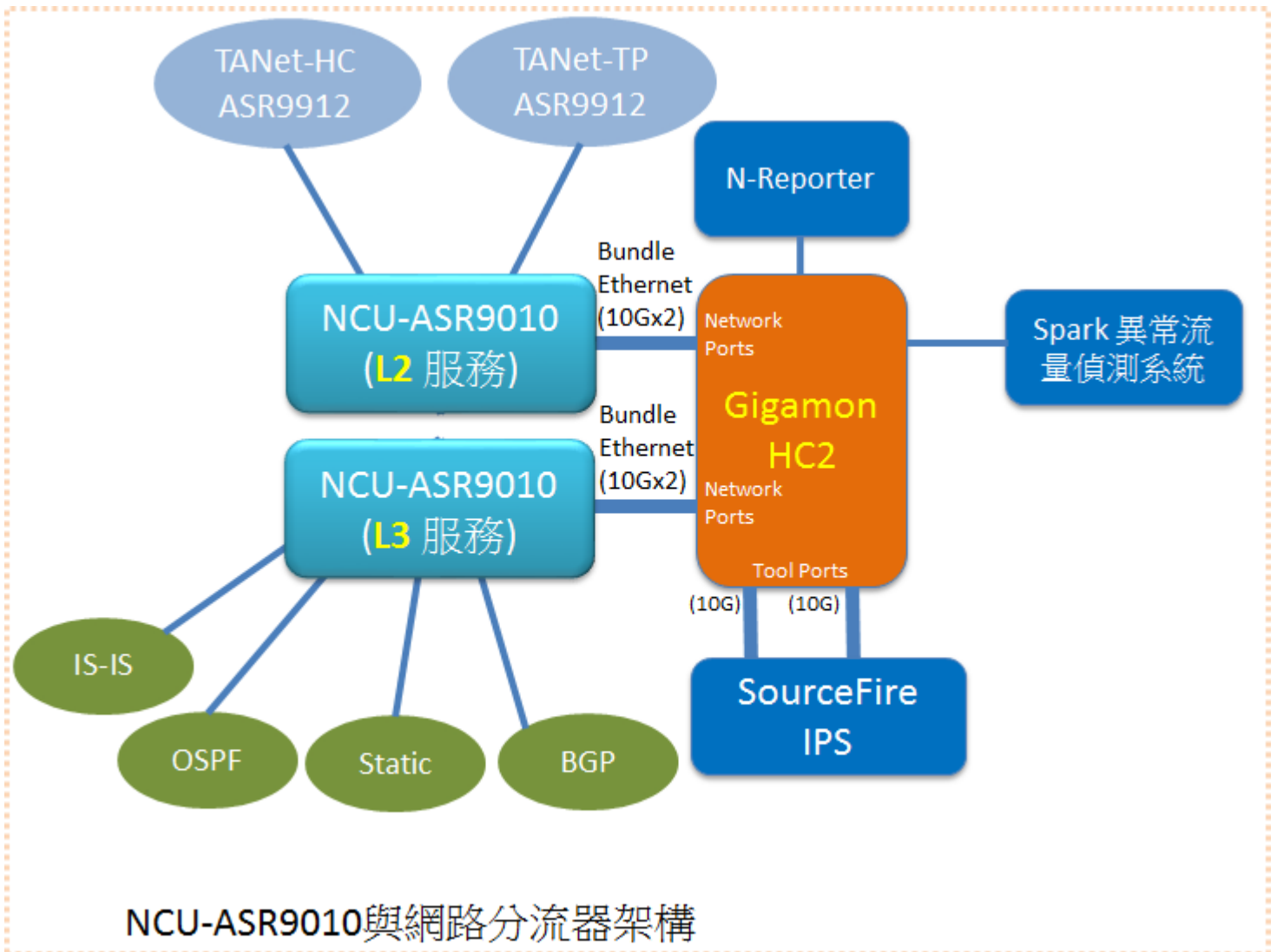
一、區網與連線單位(含縣(市)教育網路、連線學校、其他連線單位等)、TANet、

Internet(Peering)的總體架構圖



二、網路配合各種應用架構(如連線分流、頻寬管理)或資安架構(防火牆、IDS/IPS/WAF)

的規劃或實際運作架構



附表 2：連線資訊詳細表

		單位/學校名稱	電路類型	電路頻寬	電路服務商	備註
縣 (市) 教育 網中 心	1.	桃園市網	光纖	12G	中華電信 2G 亞太 10G	
	2.	連江縣網	光纖	1G	中華電信	
	3.	金門縣網	光纖	1G	中華電信	
	4.					
	5.					
大專 院校	1.	中原大學	光纖	1G	台灣固網	
	2.	元智大學	光纖	1G	中華電信	
	3.	銘傳大學	光纖	1G	中華電信	
	4.	萬能大學	光纖	10G	中華電信	
	5.	開南大學	光纖	1G	中華電信	
	6.	中央大學	光纖	10G	中華電信	
	7.	國防大學	光纖	1G	中華電信	
	8.	中央警察大學	光纖	100M	中華電信	
	9.	健行科技大學	光纖	1G	中華電信	
	10.	體育大學	光纖	200M	中華電信	
	11.	陸軍專科學校	光纖	500M	中華電信	
	12.	南亞技術學院	光纖	1G	中華電信	
	13.	國立臺北商業大學(桃 園校區)	光纖	200M	中華電信	
	14.	新生醫專	光纖	500M	中華電信	
高中 職校	1.	中壢高中	光纖	100M	中華電信	
	2.	成功工商	光纖	100M	中華電信	
	3.	治平高中	光纖	100M	中華電信	
	4.	復旦中學	光纖	100M	中華電信	
	5.	桃園農工	光纖	100M	中華電信	
	6.	育達高中	光纖	50M	中華電信	
	7.	振聲高中	光纖	100M	中華電信	
	8.	六和高中	光纖	300M	中華電信	
	9.	大華中學	光纖	100M	中華電信	
	10.	方曙中學	光纖	100M	Hinet	
	11.	大興高中	光纖	100M	中華電信	
	12.	新興高中	光纖	50M	中華電信	
	13.	永平工商	光纖	100M	中華電信	

	14.	至善高中	光纖	50M	中華電信	
	15.	啟英高中	光纖	100M	中華電信	
	16.	清華高中	光纖	50M	中華電信	
	17.	桃園美國學校	光纖	100M	接開南大學	
	18.	漢英高中	光纖	100M	Hinet	
其他 學校	1.					
	2.					
	3.					
	4.					
	5.					
其他 單位 (非 ISP)	1.	核能研究所	光纖	100M	中華電信	
	2.	資策會教育訓練處	光纖	1G	接中央大學	
	3.					
	4.					
	5.					