108 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）

108 年 11 月 21 日

目 錄

壹、基礎維運資料

一、經費及人力

1. 網路中心經費使用	(1) 核定計畫金額：**4,765,000** (2) 教育部補助金額：**3,505,000** (3) 自籌金額：**1,260,000** (4) 實際累計執行數（至 11 月）：**83%**
2. 網路中心人力數	(1).專任：3 人 (2).兼任：4 人 （請填數字）。 其中包含教育部補助： (1).網管人員：2 人，證照數：4 張。 (2).資安人員：1 人，證照數：2 張。

二、 請詳述經費使用情形及績效檢討。

年度	達成率	經費繳回原因
105 年	97.01%	
106 年	97.29%	
107 年	93.76%	繳回 73724 元，因計畫經費預估人員取得碩士學歷薪資提升，但未能在預定時間畢業。
108 年	預估 99%	

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。

網管人員(2 位)的任務配置
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。
教育部北區教育雲端資料中心相關業務
協助連線單位處理雲端服務相關問題

資安人員(1 位)的任務配置
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。

107 年計畫繳回人事費 73724 元，因計畫經費預估人員取得碩士學歷薪資提升，但未能在預定時間畢業。

四、 基礎資料(網管及資安)

請依下列項目提供本年度報告資料

(1)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	國中小學	非學校連線單位	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							單位(校)數 / 總計
(2)連線頻寬 (以電路數統計)	專線(非光纖)							
	光纖	10M(不含)以下						
		10M(含)以上 100M(不含)以下			4			4
		100M(含)以上 500M(不含)以下		5	14		8	27
		500M(含)以上 1G(不含)以下		9				9
		1G(含)以上 10G(不含)以下						
		10G(含)以上						
	其他(如 ADSL 等)							
	連線電路小計							

	縣(市)教育網路中心		連線頻寬(1)	連線頻寬(2)	備註
(3)連線縣(市)教育網路中心	1.	桃園市網	10G(亞太電信)	2G(中華電信)	
	2.	連江縣網	1G		
	3.	金門縣網	1G		

	單位名稱		連線頻寬(1)	連線頻寬(2)	備註
(4)非學校連線單位(不含 ISP)	1.				
	2.				
	3.				
	4.				
	5.				

(5)連線 TANet	臺灣學術網路(TANet)	連線台北主節點	連線新竹主節點	
		頻寬 100 Gbps	頻寬 100 Gbps	

	ISP 名稱(AS)		連線頻寬(1)	連線頻寬(2)	備註
(6)ISP 線路	1.	HINET	2G		
	2.	SeedNet	1G		
	3.	亞太線上	100M		
	4.	和信	1G		
	5.	速博	1G		
	6.	台固	1G		
	7.				
	8.				
	9.				

(7)補充說明：	
(8)連線資訊	請依附表「學校/單位連線資訊詳細表」格式填附

(2)區網中心資訊安全環境整備表

(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)	1. 1、2級資安事件處理： (1)通報平均時數：0.960小時。 (2)應變處理平均時數：0.002小時。 (3)事件處理平均時數：0.961小時。 (4)通報完成率：100%。 (5)事件完成率：99.668%。 2. 3、4級資安事件通報： (1)通報平均時數：無小時。 (2)應變處理平均時數：無小時。 (3)事件處理平均時數：無小時。 (4)通報完成率：無。 (5)事件完成率：無。 資安事件通報審核平均時數：0.829小時。
(2)網路中心配合本部資安政策。	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：96.970 %。 (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? ☑是 □否 (2)是否符合稽核要求? ☑是 □否 (3)符合資安專業證照人數：21員 (4)維護之主要網站進行安全弱點檢測比率：100%。

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)

一、108 年度網路管理維運具體辦理事項

1. 除原有 450KVA 發電機組及配電線路外，本年度新增 500KVA 發電機組 1 座。並具備切換二部發電機之開關，以確保電力不中斷。
2.建置桃園區網中心網站 http://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。
3.以 Cacti 系統即時網路流量監控, 掌控流量變化 http://cacti.tyrc.edu.tw/tyrc.html
4.計算流量 Top N 系統 ,監控大流量異常的 IP 連線
http://hadoop.tyc.edu.tw (讀取權限的帳號/密碼: tyrc /tanet_tyrc) 。
5.建置 GGC 加速 google 網站的服務 。
6.協助連線單位啟動 ipv6 連線 http://www.tyrc.edu.tw/IPV6 及監控 ipv6 mrtg 流量變化。

二、109 年度網路管理營運方針

1.持續機房維運建設(電力、空調)，維持良好網路運作。
2. 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。
3. 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。
4. 持續提供網路流量監控，並以 LINE 群組加強網路即時問題的處理。
5. 持續提供 GGC 服務。
6. 協助連線學校 IPv6 建置與推廣。

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)

一、108 年度資安服務維運具體辦理事項

1.桃園區網中心自 2010 年取得 ISO27001 認證後，每年均依規定接受複查以保持證照有效性；2019 年 3 月通過 ISO 27001:2017 改版重新驗證。提供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.本年度辦理五場資安 Workshop 實作教育訓練，課程強調動手實作以加強學習。
http://www.tyrc.edu.tw/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 106 年率先通過驗證，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 23 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）。https://pims.ncu.edu.tw/codes/index-1.php

7.108 年 2 月 15 日起，若連線單位人員無法於 24 小時內處理資安通報應變，由桃園區網中心先阻絕問題 IP 位址連線，問題解決後，再放行該 IP。

8. 桃園區域網路中心每年提供 2 次（上半年 2 月份及下半年 8 月份）資安檢測服務，服務包含以 GFI LANguard 系統進行弱點掃瞄，使用 IBM APP scan 系統進行網頁檢測

二、109 年度資安服務目標(實施措施)

1.持續推動區網中心之 ISMS 認證，並鼓勵中心同仁積極參與教育機構資安稽核觀察員之活動。

2. 推動個人資料保護制度的建立及認證。

3. 提供區域網路中心及連線學校網路資安實體環境防護機制

a. 提供區網 IPS log 分析與攻擊偵測

b. 超量攻擊之預警與阻欄

c. 協助連線學校降低疑似侵害著作權之問題事件

4. 增設高中職不當資訊過濾設備，預防學生使用學校網路會接觸到不當資訊、降低不當資訊的流竄。

5. 持續協助連線學校進行網站掃描、建檢、演練等資安相關服務。

6. 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。

7. 原每年提供 2 次資安檢測服務，自 109 年度開始，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。

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)

一、108 年度服務特色辦理成效

1. 開源軟體系統之導入與應用

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。

2019 年導入 Security Onion 系統，該系統成功地整合其他開源軟體，提供即時監控網路風險，並且提供網路入侵偵測系統及入侵防禦系統等功能。並藉由 Sguil、Squert 的 GUI 介面及警示訊息等功能，主動提供異常事件。相關導入經驗撰寫論文發表在 TANET2019 研討會，文章並以實際案例說明 Security Onion 找出挖礦主機的網路行為。

2. 雲端 Spark 異常流量偵測系統

自行開發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，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。

3. 承辦 108 年金門縣中小學網管人員校園電腦維護與管理研習

(1) 108 年 10 月 5 日(六) 9：00 ~ 16：40　由金門教育網路中心協辦，桃園區網中心率員前往金門縣教育網路中心電腦教室辦理研習。

(2) 議程表

＝＝＝＝議程表＝＝＝＝

09:00~09:10　開幕

09:10~11:10　校園網路管理

11:10~11:20　休息

11:20~12:20　網路連線分析

12:20~13:20　午餐

13:20~14:20　電腦網路安全

14:20~14:30　休息
14:30~16:30　資安檢測及弱點掃描
16:30~16:40　Q&A/賦歸
＝＝＝＝＝＝＝＝＝＝＝

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)
寬橋測試機 (2 vm)
教育媒體影音 (6 vm)
TANet VoIP (1 vm)
因材網 (1 vm)
字音字形網 (1 vm)

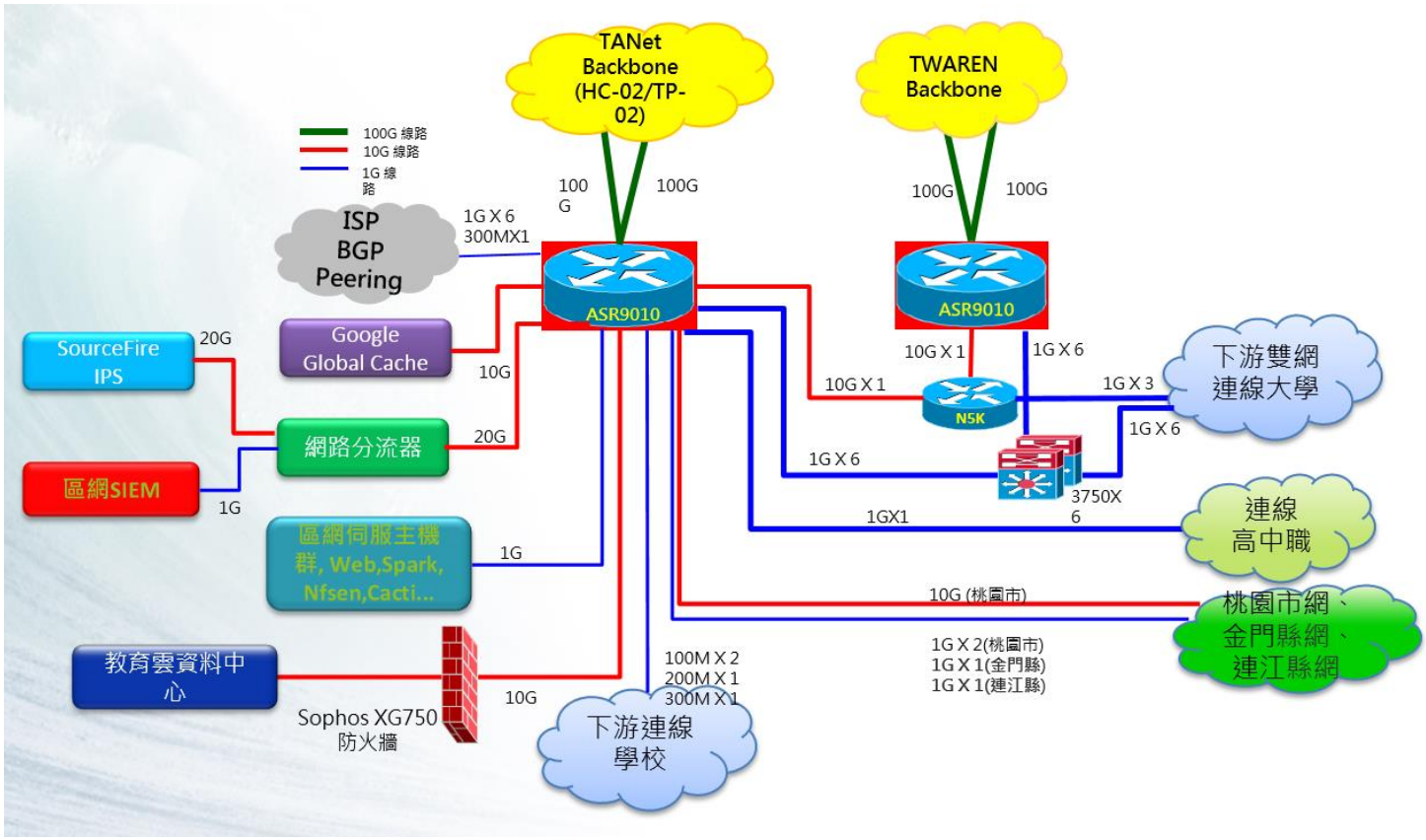
二、109 年度創新服務目標與構想
1. 辦理連線單位建議的教育訓練及研討會: 網路管理、物聯網或 AI 相關概念與應用、資安、網路智財權、資安鑑識、雲端運算。
2. 持續 Spark 異常流量偵測系統更新及對區網主幹轉送封包之監聽/分析/攻擊偵測。
3. 持續開源軟體系統之導入與應用。
4. 加強與金門及連江縣網中心合作開設離島網管資安研習課程。
5. 加強雲端服務:提供建置私有雲及教育雲服務之經驗分享/推廣。

伍、前(各)年度執行成效評量改進意見項目成效精進情形

107 年度委員建議	改進及精進做法
建置問題集	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。
對本區網中心所連接的兩個離島縣網中心,建議可思考如何提供具創新服務特色的機制,如遠距視訊應用	繼續與金門、連江縣網中心合作開設網路管理一系列課程並視需要提供遠距視訊。
資安防護技術及人才之訓練建議針對高中職負責資訊人員每年進行教育訓練,或製作影音訓練課程,供高中職負責資訊人員自行學習。	本年度開設五場資安實作 Workshop，並協助桃園市網中心辦理桃園市 108 年資訊組長研習計畫校園網路管理與網路流量分析課程。未來並配合現場環境及講師意願後將部分課程錄影以數位影音方式留存。
對區網中心維運計畫之網管及資安相關專案人員,建議應呈現其對應區網業務之績效,俾利後續能展現經費在此面上的運用效益。	本年度年終報告已加上網管及資安專案人員於區網業務之服務績效
桃園區網中心亦同時擔任北區教育雲端資料中心,建議對區網網路基礎運作機制環境評估其是否能符合資料中心對外服務效能要求。	北區教育雲以 10G 頻寬連接桃園區網核心路由器，其頻寬使用量在 1G 以下，符合其對外服務效能及未來成長需求。
資安事件處理通報平均時數為 3.924 小時,事件處理平均時數為 3.949 小時,審核平均時數為 2.035 小時,較去年退步甚多,建議了解問題處理改善之。	資安事件處理除透過自動轉通告系統即時通報連線學校，二小時未填單以電話再度通知聯繫處理情形，並針對超過 24 小時未處理的 IP 阻擋其連線。今年通報平均時數已降為 0.96 小時，審核平均時數已降為為 0.829 小時。
服務單位中有金門及連江兩個離島縣網,建議可多加了解其需求並予以協助。	今年已至金門協助研習課程，並討論後續合作開設網路管理一系列課程。
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為 97.06% ,建議加強至 100% 。	今年已加強通知，但仍有連線學校老師公務繁重，雖於 2019 年 7 月有變更密碼，但並未被列入在 8/1~10/16 統計區間內。

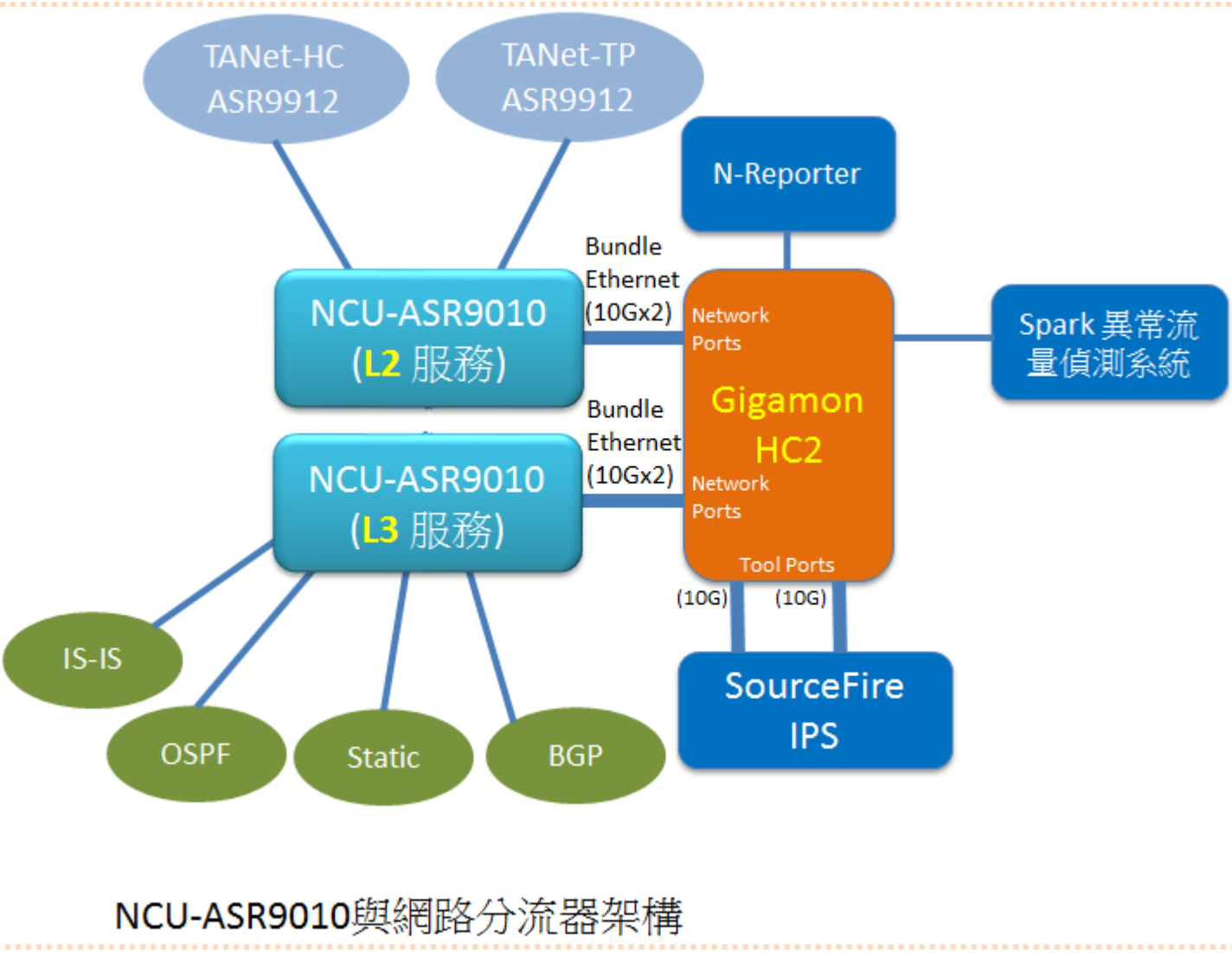
附表 1：區網網路架構圖

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



NCU-ASR9010與網路分流器架構

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	300M	中華電信	
	5.	桃園農工	光纖	300M	中華電信	
	6.	育達高中	光纖	50M	中華電信	
	7.	振聲高中	光纖	300M	中華電信	
	8.	六和高中	光纖	300M	中華電信	
	9.	大華中學	光纖	300M	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.					