南投區域網路中心
109年度年終審查

國立暨南國際大學/計算機與網路中心

報告人：陳彥良、劉育瑄

基礎維運資料-年度經費

本年度經費使用情形：

教育部核定計畫金額：140 萬元

教育部補助計畫金額： 140 萬元

區網中心自籌金額： 40 萬元 (極早期火災偵測系統)

實際累計執行數（1月-11月）：136萬元 ，執行率97%。

基礎維運資料-中心人力配置

專任：19人　　兼任：2人

其中包含教育部補助：無補助雲端管理人員

1. **網路管理 1人 證照數4張**
   - ISO 27001 資訊安全管理系統、BS 10012個人資料管理系統、網路架設丙級、職能評量證書-資通系統風險管理
2. **資安管理 1人 證照數7張**
   - ITE 網際網路介接基礎、ITE 資料通訊、ITE 網路安全、ITE 網際網路服務與應用、網路架設乙級技術士技、CHFI 資安鑑識調查專家認證、職能評量證書-網路架設與部署安全

基礎維運資料-年度經費

歷年經費使用情形：

年度	核定補助經費	年度達成率	備註
106	1,350,000	99.89%	經費無須繳回
107	1,390,000	100%	經費無須繳回
108	1,395,000	99.95%	經費無須繳回
109	1,400,000	97%	本年1-11月

基礎維運資料-人力

人員任務配置：

在職年度	職稱	姓名	人員配置
98年-迄今	網管人員	劉育瑄	骨幹網路監測及故障排除 資安事件之通報、應變、審核及事件資料收集與分析 計畫經費控管及計畫行政業務 ISMS 系統導入及驗證、資通安全法導入 區網網頁管理 配合教育部進行資安通報演練、社交工程演練 舉辦教育訓練及相關活動 IPv6推廣 提供連線單位各事項反應及聯絡窗口及其他交辦事項
103年-迄今	資安人員	陳彥良	骨幹網路監測及故障排除 資安事件之通報、應變、審核及事件資料收集與分析 防火牆管理，阻擋 DDoS 攻擊，降低 DDoS 對網路服務的影響 配合教育部進行資安通報演練、社交工程演練 協助弱點掃描 機房環境監測及電力設備維護 提供連線單位技術協助及其他交辦事項

基礎維運資料-人力

人事經費運作情形：

年度	核定人事費	人事費餘額	備註
106	1,248,962	23	經費無須繳回
107	1,294,387	452	流用至業務費 經費無須繳回
108	1,316,208	694	經費無須繳回
109	1,328,605	0	經費無須繳回

基礎維運資料-網路及資安管理

區域網路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	非學校之連線單位(不含ISP)	總計
下游連線學校或連線單位數統計	連線學校(單位)數	1	2	10	1	9	連線單位總數 23
	連線單位比例	1/23	2/23	10/23	1/23	9/23	註：單位數 / 總數

基礎維運資料-網路及資安管理

區域網路中心連線資訊彙整表：

連線頻寬與電路數統計	專線(非光纖)						
	光纖	10M(不含)以下		1			1
		10M(含)以上100M(不含)以下					1	1
		100M(含)以上 500M(不含)以下			12	1	8	21
		1G(含)以上 10G(不含)以下	4					4
		10G(含)以上		2				2
	其他(如ADSL等)							
	連線電路小計		4	3	12	1	9	29
	連線頻寬合計 (電路實際租用頻寬加總)		4096m	20485m	1200m	100m	820m	連線頻寬總計： 26701m
	連線頻寬比率		15.34%	76.72%	4.49%	0.37%	3.07%	請加總電路實際租用頻寬/總計頻寬

基礎維運資料-網路及資安管理

區域網路中心連線資訊彙整表：

連線縣(市)教育網路中心	縣(市)教育網路中心		連線頻寬		合計
	1.	南投縣教育網路中心	連線頻寬(1)	中華電信1G×2	4G
			連線頻寬(2)	亞太電信1G×2	
非學校之連線單位(不含ISP)	連線單位名稱		連線頻寬		備註
	1.	台大清水溝	100M		
	2.	台大溪頭	100M		
	3.	台大下坪植物園	100M		
	4.	台大水里	100M		
	5.	台大內茅埔	100M		
	6.	台大和社	100M		
	7.	台大水里營林區	100M		
	8.	台大竹山	20M		
	9.	台大對高岳營林區	100M		

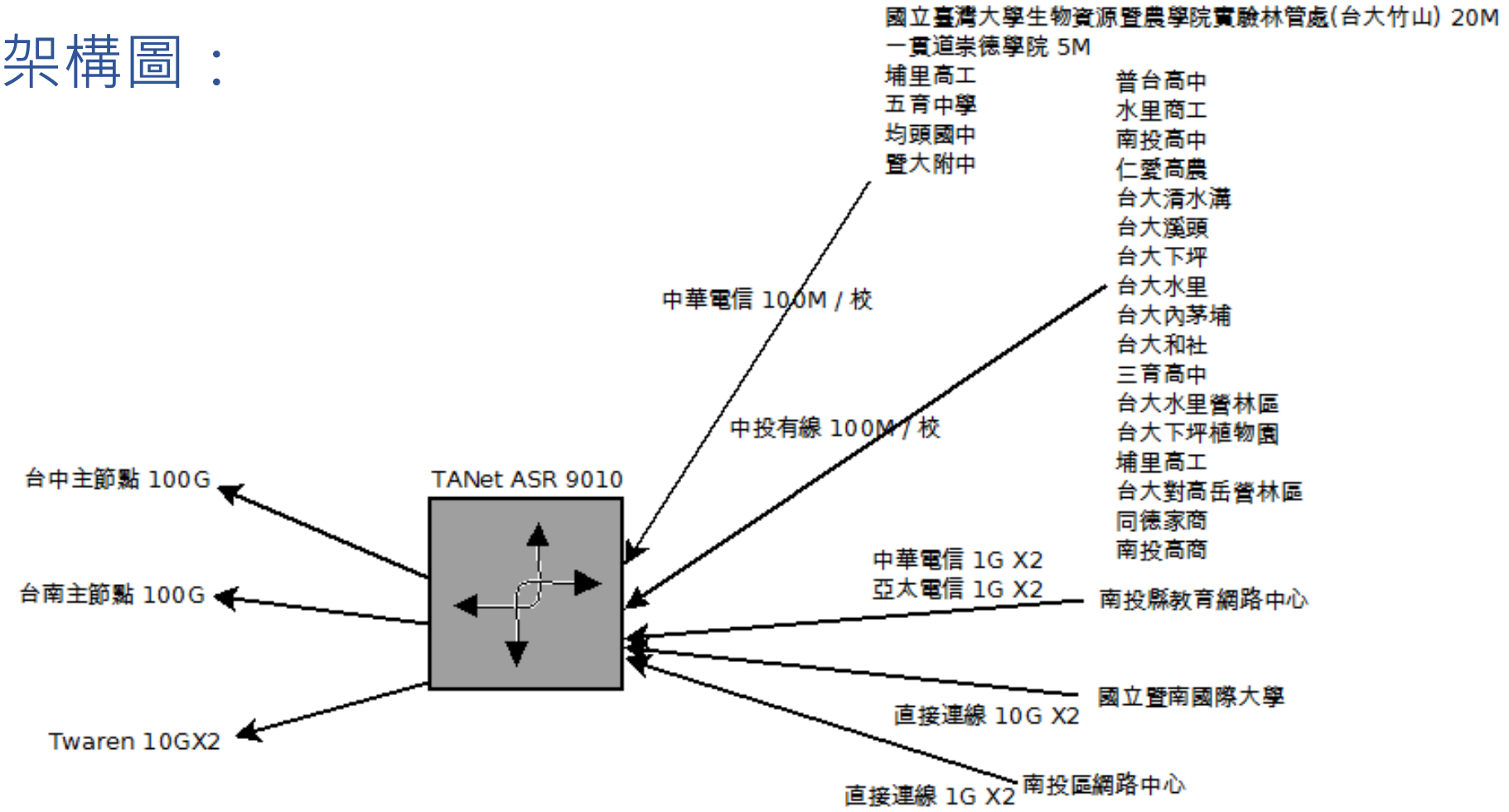
基礎維運資料-網路及資安管理

區域網路中心連線資訊彙整表：

		主節點名稱	連線頻寬	備註
連線TANet	1.	台中主節點	100G	
	2.	台南主節點	100G	

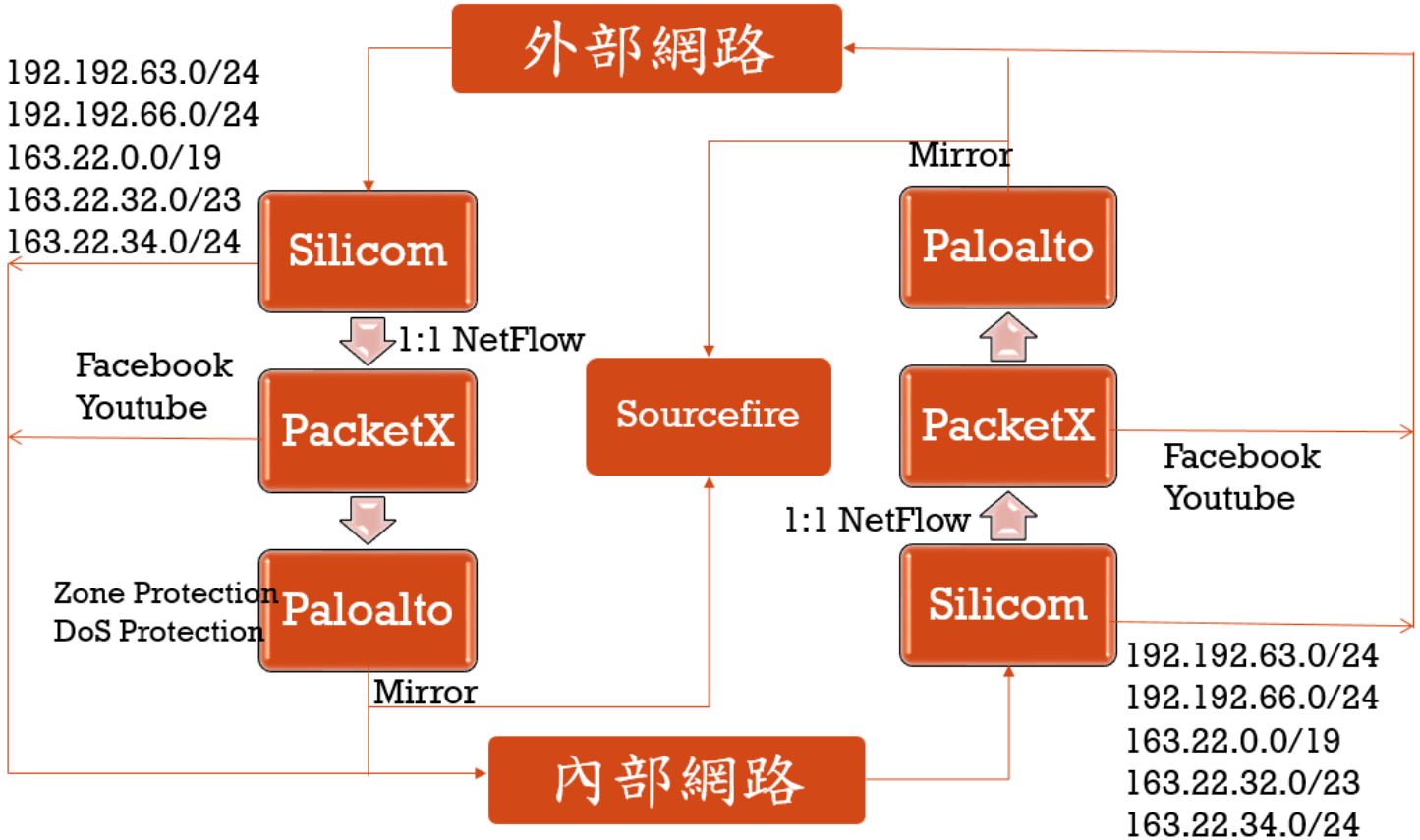
基礎維運資料-網路及資安管理

網路架構圖：



基礎維運資料-網路及資安管理

網路資安架構圖：



基礎維運資料-網路及資安管理

區域網路中心資訊安全環境整備表：

區域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

1、2級資安事件處理：

1) 通報平均時數：0.09小時
2) 應變處理平均時數：0小時
3) 事件處理平均時數：0.6小時
4) 通報完成率：100%
5) 事件完成率：100%

資安事件通報審核平均時數：1.07小時。

本年度並無3、4級資安事件

基礎維運資料-網路及資安管理

區域網路中心配合本部資安政策：

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 100 %

本中心符合

✓資通安全防護縱深要求

具備防毒、防火牆、郵件過濾系統、IDS/IPS

✓稽核要求

通過教育體系資訊安全認證

✓資安專業證照人數達8人（ ISO27001 主導稽核員證照）

✓維護之主要網站進行安全弱點檢測比率：100%

區網網站定期進行弱點掃描並進行修補

具體辦理事項-網路管理

109年度網路管理維運具體辦理事項：

✓持續提供NetFlow查詢系統並開放給連線單位使用

N-Reporter收集1:1 NetFlow資訊，可提供精確且詳細資料供連線單位自行查詢，並有統計各單位流量排名等功能，當流量雍塞時找出異常使用IP。

✓提供cacti可回溯的流量紀錄與查詢

可查詢各連線單位每日、每星期、每月、每年等區間的統計流量，網頁連結https://www.ntrc.edu.tw/cacti/traffic3.html。

具體辦理事項-網路管理

109年度網路管理維運具體辦理事項：

✓What's Up監測:

監測骨幹與連外反應狀態，包含骨幹路由器ASR9101、骨幹防火牆Paloalto5060、骨幹分流設備PacketX、機房UPS，另外針對網路有偵測台中主節點、台南主節點、與各連線單位節點狀態，可提供可用率(Availability) 、回應時間(Response Time)與斷線告警。

✓分流設備:目前有三個主要作用

- 過濾加密流量進入資安設備降低資安設備負擔。
- 產生1:1 NetFlow。
- 將流量拆解分別送入兩台ASOC所架設的FirePower中做異常行為偵測。

具體辦理事項-網路管理

109年度網路管理維運具體辦理事項：

✓協助遠距課輔軟硬體及網路維護，及維持課輔品質。

✓IPv6推動：建置IPv4/IPv6 Dual-Stack環境，持續推廣IPv6 服務（今年4月至迄今）。

✓召開連線單位管理委員會，已於本年7/6日召開第一次管理委員會，預計於12月8日召開第二次管理委員會

具體辦理事項-網路管理

109年度網路管理維運具體辦理事項：

✓舉辦教育訓練研討會

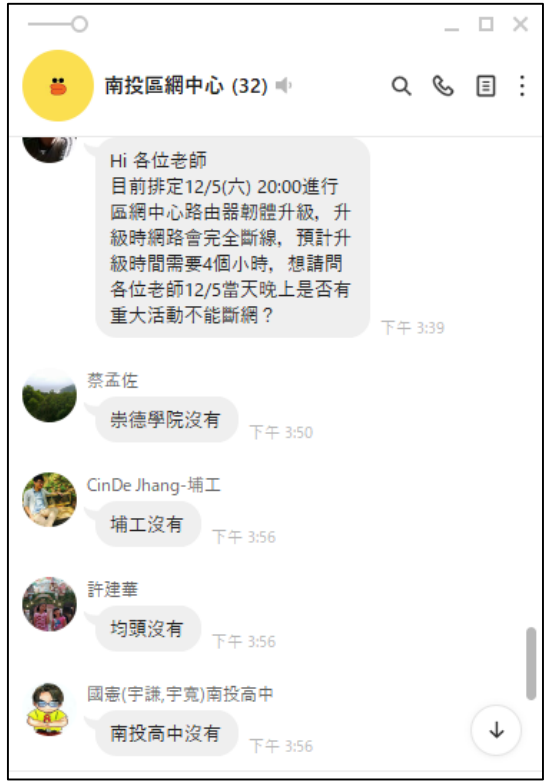
於7/6日舉辦資安教育訓練，議題分別為IPv4/IPv6 雙協定網路建置經驗分享、資訊安全面面觀。

於10/26與南投縣網中心受台中市政府教育局「教育體系單一簽入服務推廣計畫」委託辦理南投縣高中職校單一簽入服務登入各項應用服務之教育訓練。

具體辦理事項-網路管理

109年度網路管理維運具體辦理事項：

- ✓區網首頁公告資安相關資訊，包含區網研討會資訊、資安相關議題及新聞，首頁資訊如連結https://www.ntrc.edu.tw/。
- ✓資通安全相關議題討論及分享。
- ✓建置連線單位LINE群組，提供便捷快速的分享及交流空間。



具體辦理事項-網路管理

110年度網路管理營運方針：

(一)持續提供NetFlow查詢系統。

(二)持續提供cacti可回溯的流量紀錄與查詢。

(三)持續推廣IPv6 Dual-Stack環境，實地網路環境訪視及現況訪談6間連線單位，並持續建置網頁取樣統計點。

(四)召開2次管理委員會。

(五)舉辦資安或推廣IPv6 相關教育訓練至少1場次。

具體辦理事項-資安服務

109年度資安服務維運具體辦理事項：

✓參與北區ASOC中心計畫區網建置兩台FirePower入侵防禦系統，並透過TACERT台灣學術網路危機處理中心平台派發資通安全事件。

✓骨幹防火牆，主要進行流量過濾與惡意清單封鎖，並針對基本DoS攻擊進行阻擋達到第一道防線的功能。

✓網頁弱點掃描，本中心每年幫連線單位進行兩次網頁弱掃服務，本年度許多連線單位為配合政策將網頁進行向上集中，故協助連線單位修改網頁後再次弱掃服務。

具體辦理事項-資安服務

109年度資安服務維運具體辦理事項：

✓機房環控監測：

- 門禁：本中心依ISMS規定進行機房門禁管制。
- 溫濕度：本中心依ISMS規定機房溫濕度，機房溫濕度異常時將會發出簡訊及電子郵件告知。
- 漏液偵測：機房內設有漏液偵測設備，當漏水時可以第一時間發簡訊告警通知維運人員。
- 機房消防：於骨幹區與UPS室設有獨立偵煙設備，當發生火災時會以簡訊通知維運人員。
- UPS 不斷電系統：機房UPS緊急供電能力達1.5小時，並一季做一次基礎保養及放電測試。
- 市電及發電機保養：每年7月進行重電保養確保電力系統穩定供電，另設有電力監測系統，當發生市電中斷會第一時間發簡訊告警。

具體辦理事項-資安服務

109年度資安服務維運具體辦理事項：

✓ISMS驗證導入

本中心持續通過教育體系資通安全驗證，由於資通安全法規定A、B級機關需通過公正符合國家標準的第三方驗證（例如：ISO27001），故預計110年改導入ISO27001並通過其驗證。

具體辦理事項-網路管理

110年度資安服務目標：

(一)持續參加ASOC 中心計畫。

(二)持續骨幹防火牆主要進行流量過濾與惡意清單封鎖。

(三)每年協助連線單位網頁進行2次弱點掃描，必要時連線單位可提出增加掃描次數。

(四)提供諮詢及協助連線單位導入ISMS及完成資安法所要求規定事項。

(五)導入ISO27001，並提出驗證申請。

(六)持續執行109年度項目。

未來營運計畫-特色服務

109年度服務特色辦理成效：

IPv6推廣服務將協助連線單位建置IPv4/IPv6 Dual-Stack環境，例如：校首頁支援IPv6程度、DNS IPv6相關設定、IPv6網段分配及管理建議、IPv4/IPv6資安軌跡紀錄及收集、IPv6相關教育訓練等..

連線單位14間（不包含台大實驗林分部）		
項目	完成間數	完成率
實地環境現況及訪談	8	57%
區網端IPv6 設定	14	100%
Web Server IPv6設定	10	73%
Web Server支援IPv6正解	10	73%
網頁取樣分析	5	33%

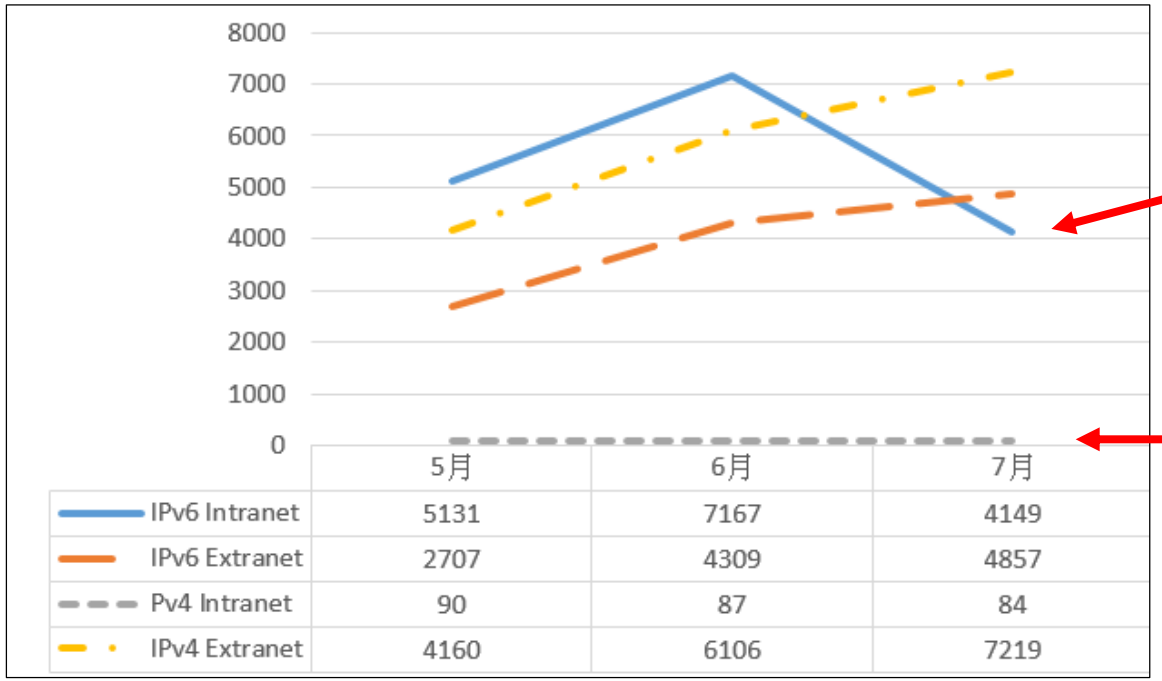
南投區網中心 連線單位	主要 Web Server	Web Server是否支援IPv6 連線	Web Server是否支援IPv6 正解
南投區網中心	https://www.ntrc.edu.tw	✔	✔
國立暨南國際大學	https://www.ncnu.edu.tw	✔	✔
崇德一貫道學院	http://www.iktcds.edu.tw	✘	✘
國立埔里高級工業職業學校	http://www.plvs.ntct.edu.tw	✔	✔
國立暨南國際大學附屬高級中學	http://www.pshs.ntct.edu.tw	✔	✔
私立普台高級中學	http://www.ptsh.ntct.edu.tw	✘	✘
國立水里高級商工職業學校	https://www.slvs.ntct.edu.tw	✔	✔
國立南投高級中學	https://www.ntsh.ntct.edu.tw	✔	✔
私立同德高級家事商業職業學校	http://www.tdvs.ntct.edu.tw	✘	✔
國立仁愛高級農業職業學校	https://www.ravs.ntct.edu.tw	✔	✔
三育高級中學	http://www.taa.ntct.edu.tw	✔	✔
五育高級中學	http://site.wu-yu.ntct.edu.tw	✘	✘
國立南投高級商業職業學校	http://www.pntcv.ntct.edu.tw	✔	✔
均頭國中	http://www.jtjhs.ntct.edu.tw	✔	✔
台大溪頭實驗林	https://www.exfo.ntu.edu.tw	✔	✔
2020 08 14 15:37:11			

Web Server IPv6設定及Web Server支援IPv6正解

未來營運計畫-特色服務

109年度服務特色辦理成效：舉例其中一項統計分析案例

✓仿照APNIC的統計方式，放置連結至各校校首頁，來進行校內、外 IPv4/IPv6 的裝置連線校首頁數統計



	5月	6月	7月
IPv6 Intranet	5131	7167	4149
IPv6 Extranet	2707	4309	4857
Pv4 Intranet	90	87	84
IPv4 Extranet	4160	6106	7219

IPv6校內連線數

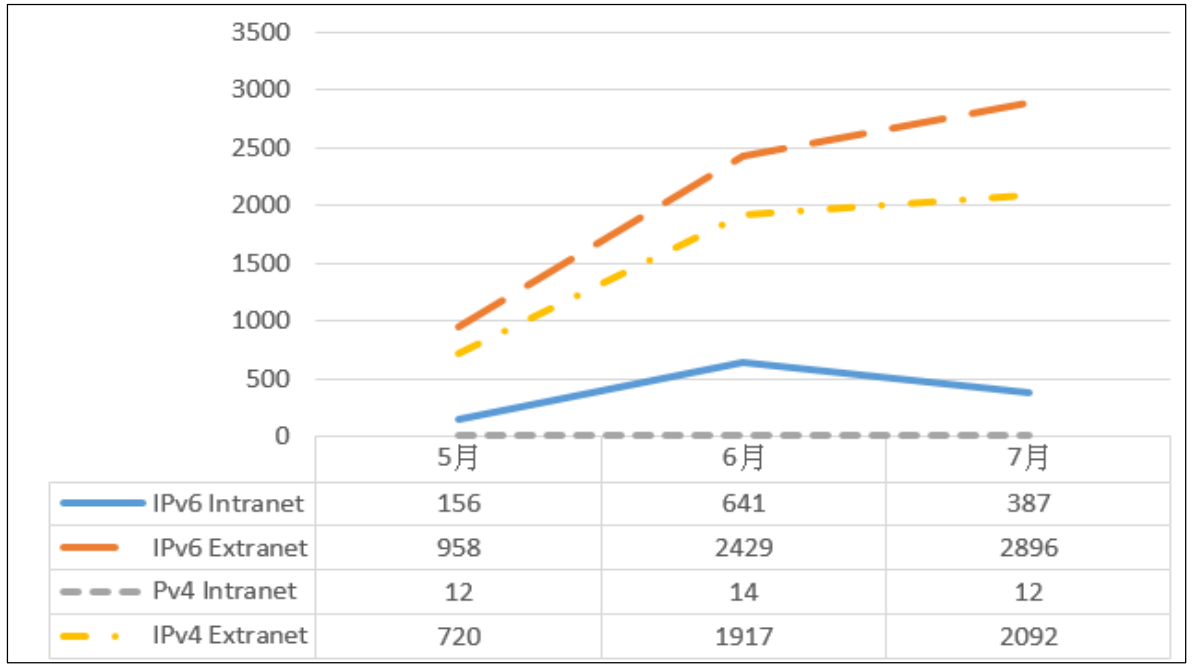
IPv4校內連線數

網頁取樣分析-暨大校首頁

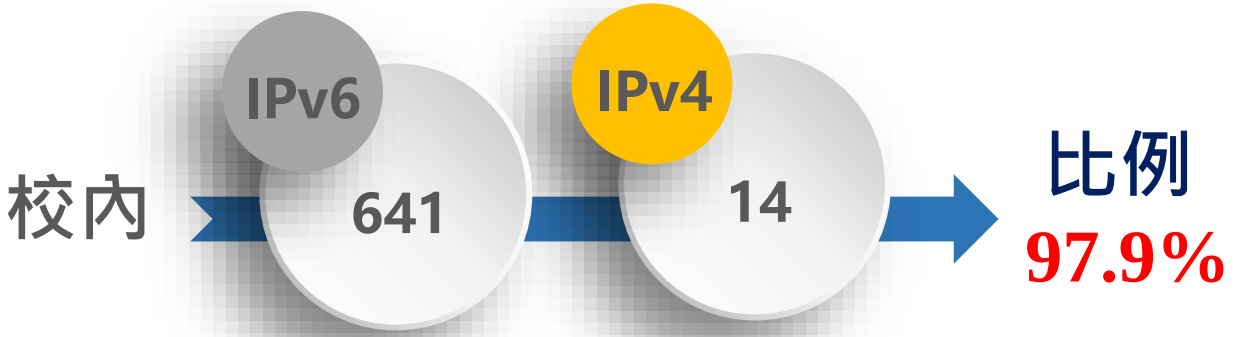
未來營運計畫-特色服務

109年度服務特色辦理成效：舉例其中一項統計分析案例

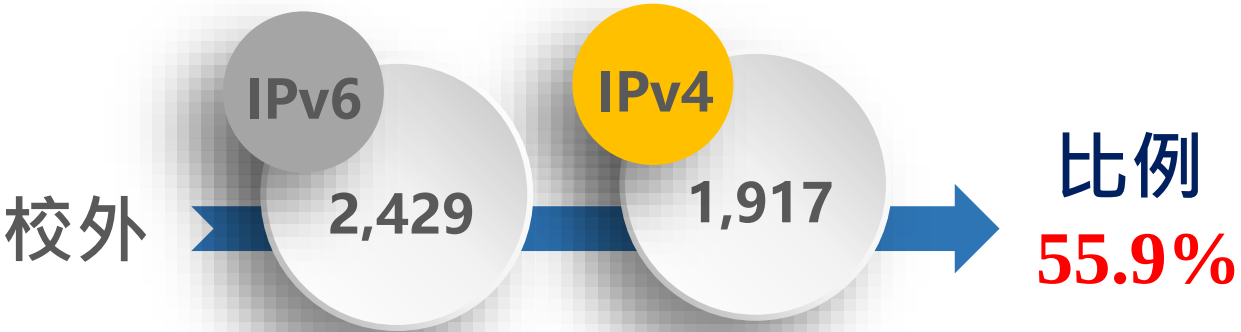
連線單位-某高職



	5月	6月	7月
IPv6 Intranet	156	641	387
IPv6 Extranet	958	2429	2896
Pv4 Intranet	12	14	12
IPv4 Extranet	720	1917	2092



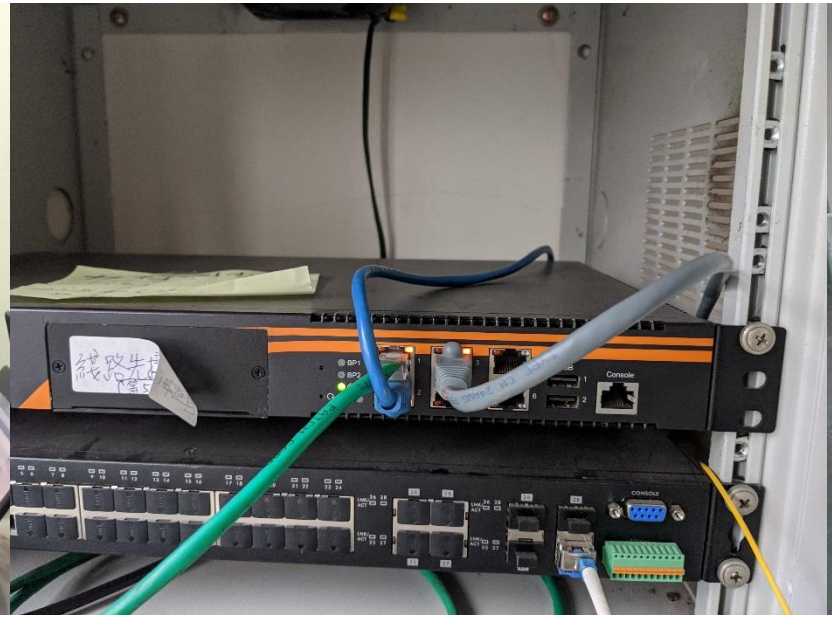
可見某高中校內的 IPv6 基礎建置完整。



未來營運計畫-特色服務

109年度服務特色辦理成效：

協助偏鄉課輔計畫，小學端及大學端電腦教室硬體、軟體及網路環境維護，服務的單位有 都達國小、法治國小、仁愛國小、力行國小及瑞峰國中。



未來營運計畫-特色服務

109年度服務特色辦理成效：

綠色機房建置：暨南大學海拔665公尺，夏季溫度介於32~24℃，冬季介於23~15℃，寒流來襲甚至低於10℃以下，在如此條件下，實施節能減碳規劃，冬季將採外氣引入機制，在氣溫低於20℃時啟動外氣引入，此系統為一台5HP馬力的鼓風機及其外側設置3層濾網，搭配80*40公分風管，將外部冷空氣均勻導引機房內，目前中心機房整年度PUE值可達1.22~1.62。

未來營運計畫-特色服務

109年度服務特色辦理成效：

✓資安法推動，因應資安法要求分享ISMS導入經驗及施行細則要求執行事項討論。

✓協助連線單位資安通報事件查詢：針對連線單位資安通報進行各別分析，並將分析結果與可行解決方法告知單位承辦人員，降低被重複通報機率。

MALWARE-CNC Win.Trojan.Gh0st variant outbound connection	175.183.62.229 為站點防火 163.22.186.196 為unifi wifi a 正常傳輸	誤報
MALWARE-CNC Win.Trojan.Agent variant outbound connection	ams 字串	應該為誤報
MALWARE-CNC Win.Adware.Taplika toolbar download attempt	start.mysearchdial.com	https://malwaretips.com/blogs/start-mysearchdial-removal/
MALWARE-CNC Win.Adware.Taplika toolbar download attempt	start.mysearchdial.com	已請老師移除程式
MALWARE-CNC Win.Adware.Taplika toolbar download attempt	start.mysearchdial.com	
MALWARE-OTHER Trackware relevantknowledge runtime detection	User-Agent: OSSProxy 1.3.338.320 Host: rules.securestudies.com https://www.hybrid-analysis.com/sample/4f903d8a4abefdf94b17d16c46490acfe91f84f8bbe74156f9974e http://cleanbytes.net/relevant-knowledge-what-is-it-how-it-get-installed-and-how-to-remove-it https://user-agents.net/string/ossproxy-1-3-338-320-build-338-320-win32-en-us-apr-9-2020-18-44-54	

未來營運計畫-特色服務

110年度創新服務目標與構想：

✓持續IPv6推廣服務將協助連線單位建置IPv4/IPv6 Dual-Stack環境。

✓持續協助偏鄉課輔計畫小學端及大學端電腦教室硬體、軟體及網路環境維護。

✓機房將採購極早期火災偵測系統，並搭配既有外氣引入系統規劃建置。

✓持續協助連線單位資安通報事件查詢。

前年度改進意見項目及成效精進情形

108年委員精進建議項目	109年精進建議改進情形
網路中心及連線學校資安事件緊急通報處理之通報平均時數及事件處理平均時數均超過 1 小時，事件完成率皆未達 100%，尚須努力。	本年度通報應變時數已精進 (1) 通報平均時數：0.09小時。 (2) 應變處理平均時數：0小時。 (3) 事件處理平均時數：0.6小時。 (4) 通報完成率：100%。 (5) 事件完成率：100%。
自籌 320 萬購置更換防火牆，使網路環境更完整，但只服務暨南大學本身。區網之防火牆已老舊，建議予以強化與正面處理; 資安設備因授權權限問題，設備無法充分運用，建議盡量原規劃購置時多加考量避免資源浪費。	礙於預算問題目前尚未購置區網防火牆，但108年暨大自籌購置防火牆後，透過區網分流器設定，使暨大流量不經區網防火牆（僅有縣網及連線單位），可降低區網防火牆負擔。

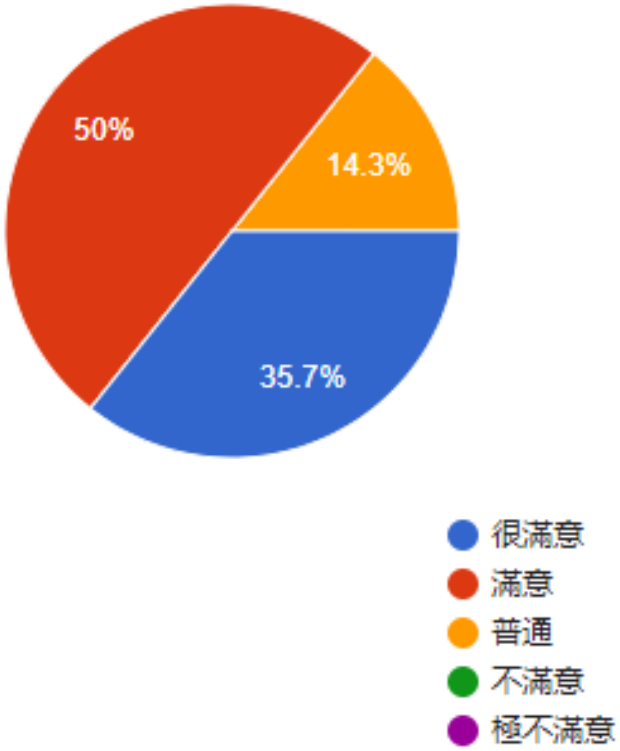
前年度改進意見項目及成效精進情形

108年委員精進建議項目	109年精進建議改進情形
區網中心之運作僅維持基本穩定之服務，建議可參考其他區網辦理之特色，引進相關服務，以造福連線學校。	本年度積極推廣IPv4/IPv6 Dual-Stack環境建置並實地至連線單位訪談、協助設定及技術諮詢，部分學校已完成IPv4/IPv6 Dual-Stack環境建置及網頁支援IPv6等相關設定。
有關資訊安全之一般人員須 3 個小時之教育訓練，建議區網可以協助連線學校審慎辦理。 區網中心之責任包括加強對縣市網路中心及連線單位之主動協處服務，應多多給於連線單位提供適時協助	本年度已於於7/6日舉辦資安教育訓練，共計時數6小時。 與南投縣網中心一同舉辦「教育體系單一簽入服務推廣計畫」南投場次，縣網中心負責2場次共計6小時，區網中心負責1場次共計6小時。
宜落實管理委員會的功能，並對於區縣網的合作以及對連線學校的服務提出更積極的作法	已於7/6日第一次管理委員會，預計於12月8日召開第二次管理委員會。

滿意度調查

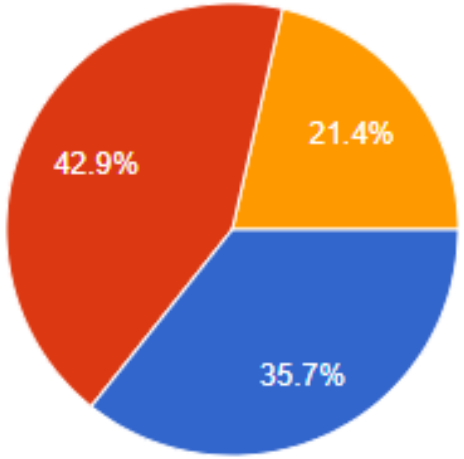
電信業者(ISP)線路穩定度

滿意度



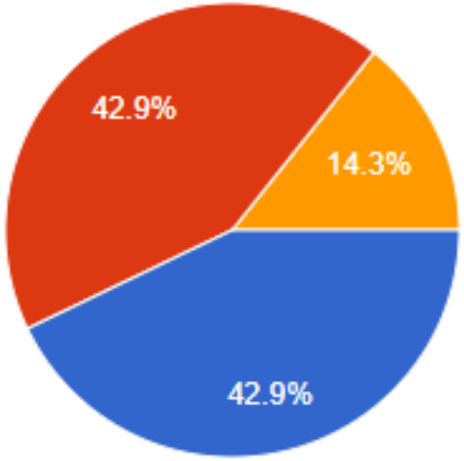
電信業者(ISP)維修速度

滿意度



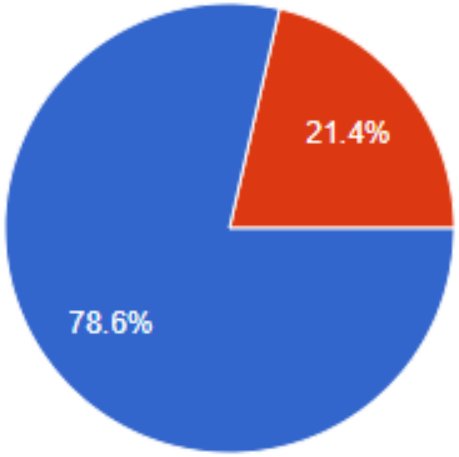
電信業者(ISP)服務態度

滿意度

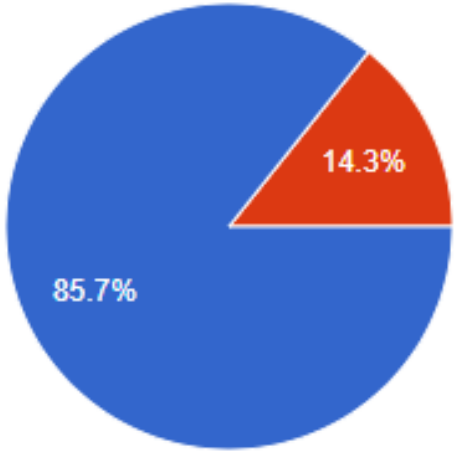


滿意度調查

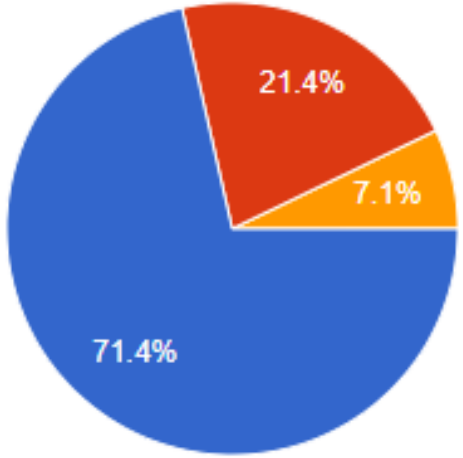
協助處理資安通報時效滿意度



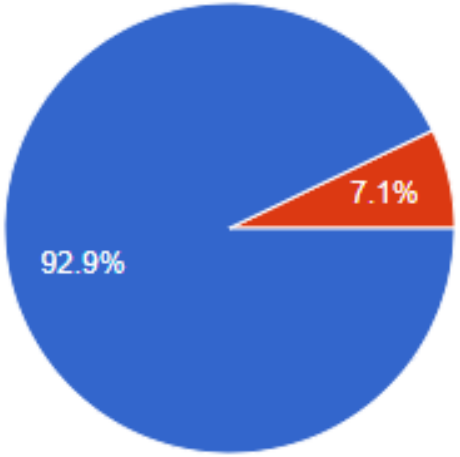
協助處理問題及障礙排除滿意度



教育訓練議程安排滿意度



區網人員整體服務滿意度



報告結束

感謝大家聆聽