111 年度區域網路中心年終成果基礎資料彙整表

臺北 I 區域網路中心

（負責學校：國立臺灣大學）

111 年 11 月 8 日

目錄

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

區域網路中心經費使用	1. 教育部核定計畫金額：新臺幣 **1,792,000** 元 2. 教育部補助計畫金額：新臺幣 **1,792,000** 元 3. 區域網路中心自籌額：新臺幣 **0** 元，補助比率 0 %。 4. 實際累計執行數(1 月至 10 月)：新臺幣 **891,578** 元，執行率 50%。
區域網路中心人力運作	專任： **2** 人，兼任： **0** 人。 其中包含教育部補助： 1. 網路管理人員： **1** 人，證照數： **1** 張。 2. 資安管理人員： **1** 人，證照數： **1** 張。 3. 雲端管理人員：＿＿＿＿人，證照數：＿＿＿＿張。(無者免填)

二、請詳述歷年度經費使用情形與績效檢討。

說明: 1.請填寫前 3 年度(108-110)經費使用達成率及本(111)年度預計達成率。
2.檢討歷年度達成率。(如有經費繳回，請述明原因)。

年度	教育部核定	實支總額	人事費繳回	達成率	扣除繳回達成率
107	1,720,000	1,577,987	51,040	91.74%	95%
108	1,720,000	1,714,788	5,097	99.69%	99.99%
109	1,620,000	1,548,009	6,7841	96%	96%
110	1,792,000	1,788,692	0	99.82%	99.82%
111	1,792,000	891,578 (10月底)		70% (預估)	98% (預估)

109 年因新聘網路助理薪資級距與前任不同，人事費部分繳回
110 年網路與資安助理皆是滿聘，因此達成率達 99.82%
111 年預估達成率僅 70%，因資安助理 4/31 離職，至今尚未找到合適人選

三、請詳述教育部補助貴區網中心之網管、資安及雲端人力的服務績效。

說明: 1.請填寫前 3 年度(108-110)及本(111)年度人員配置及異動情形。
2.檢討歷年度人事經費運作(如人事經費有繳回，請述明原因)。

甲、網管人員人力規劃一名，工作執掌如下:

1.臺北區網網路中心 I 網路管理維運。

2.網路服務品質分析與監控。

3.區網雲端租賃服務管理維運。

4.連線單位網路故障與排除。

乙、資安人員人力規劃一名，工作執掌如下:

1.資安事件通報與處理。

2.資安事件鑑識與調查。

3.DDoS 異常通報與回覆

4.網路異常分析與監控。

丙、檢討歷年度人事經費運作

1.109 年因新聘網路助理薪資級距與前任不同，人事費部分繳回

2.110 年網路與資安助理皆是滿聘，因此達成率達 99.82%

3.111 年預估達成率僅 70%，因資安助理 4/31 離職，至今尚未找到合適

人選

四、112 年度經費與人力營運規劃(預估)。

甲、112 年經費規劃:

教育部補助計畫項目經費

申請單位: 國立臺灣大學

計畫期程： 112 年 1 月 1 日至 112 年 12 月 31 日

計畫經費總額：1,902,990 元，向本部申請補助金額：1,902,990 元，自籌款： 元

擬向其他機關與民間團體申請補助：▓無□有

（請註明其他機關與民間團體申請補助經費之項目及金額）

教育部： 元，補助項目及金額：

XXXX 部：.....元，補助項目及金額：

經費項目		計畫經費明細			
		單價（元）	數量	總價(元)	說明
一、人事費	專任行政助理薪資(網管)	39,507	8	316,056	1.薪資預算含年終獎金 1.5 個月。 2.第二年碩士薪資
		40,503	5.5	222,767	
	行政助理勞保費雇主(網管)	3,284	8	26,272	2. 勞健保、勞退費用依勞基法規定辦理。 3.依僱員年資計算，薪資將於 110 年 6 月 1 日提敘一級。 4.專任助理未依上述經費聘用人員致所餘經費不得流用，應依補助比率繳回 。 5.補(捐)助計畫專任助理如確有加班事實，加班費不得由補(捐)助經費支給，惟仍應依勞動基準法規定辦理，並由執行單位年度經費核實支給加班費。
		3,439	4	13,756	
	行政助理健保費雇主(網管)	1,965	8	15,720	
		2,058	4	8,232	
	行政助理勞退雇主(網	2,406	8	19,248	

	管)	2,520	4	10,080	
	二代健保補充保費(網管)	1,282	1	1,282	年終獎金 2.11%之二代健保補充保費。二代健保補充保費為 40,503*1.5*2.11%=1,282
	專任行政助理薪資(資安)	46,674	13.5	630,099	1. 薪資預算含年終獎金 1.5 個月。 2. 第九年碩士薪資
	行政助理勞保費雇主(資安)	3,750	12	45,000	1 .勞健保、勞退費用依勞基法規定辦理。 2.為延攬聘任稀少性、技術性人員，若該員通過本校特殊性等助理申請審核，於補助計劃預算內給予加計資訊專業加給依僱員年資計算。 3.專任助理未依上述經費聘用人員致所餘經費不得流用，應依補助比率繳回 。 4.補(捐)助計畫專任助理如確有加班事實，加班費不得由補(捐)助經費支給，惟仍應依勞動基準法規定辦理，並由執行單位年度經費核實支給加班費。
	行政助理健保費雇主(資安)	2,362	12	28,344	
	行政助理勞退雇主(資安)	2,892	12	34,704	
	二代健保補充保費(資安)	1,477	1	1,477	年終獎金 2.11%之二代健保補充保費。二代健保補充保費為 46,674*1.5*2.11%=1,477。
			小計	**1,373,037**	
二、業務費	講座鐘點費	2,000	30	60,000	依據「講座鐘點費支給表」之規定，外聘專家學者 2,000 元，1 場 3 小時。預計舉辦 10 場，共 60,000 元。
	講座鐘點費補充保費	42	30	1,260	依二代健保規定，須支 2.11%補充保費元。 2000 元*2.11%=42 元 42 元*30 小時=1260 元
	工讀費	168	432	72,576	因應特色區網中心維運業務需求，以臨時人力支應各項業務。 1.辦理各類會議、講習訓練與研討（習）會、網頁或資料庫維護與更新、資訊安全作業等，所需臨時人力。 2.TANet 網頁、資料庫建立與維護-臨時人力需求時數(以學習型助理支應)，每月 36 小時，共 36*12=432 小時。 3. 依本校臨時人員薪資規範支給。
	交通費	1,500	5	7,500	參加會議校內同仁或來訪學者專家、講師之旅、運費，單程以 1,500 元估算，預估 5 人次來回為 1,500*5=7,500 元。 依國內出差旅費報支要點辦理。

	膳宿費	2,000	3	6,000	依國內出差旅費報支要點辦理，外出參與會議之住宿費，預估為 3 人次。2,000*3=4,800 元
		140	500	70,000	辦理研習會、座談會或訓練進修，預估 10 場，每場 50 人次。(誤餐費 100+茶點費 40)
	維護運作：辦公室電信費、水費、電費	699	12	8,388	處理區網事務及回覆 TACERT 資安事件通訊費用，月租費 699 元*12 個月。
	設備維護費	3,000	12	36,000	區網中心相關主機等維護費，預計每月約 3000 元*12 個月，以 24,000 元計。
		5,000	12	60,000	SIP 伺服器維護費，預計每月約 5,000 元*12 個月，以 60,000 元計。
	電腦、通訊、周邊設備之介面、零件	6,000	1	6,000	區網中心設備維護費及其他網路運作相關網路資訊材料(單價未達 10,000 元之非消耗品)
	專業證照、教育訓練費	80,000	1	80,000	人員專業技術培養，以提升區網維運技能及服務品質。教育訓練、證照考取等費用支出。
	雜支	2,229	1	2,229	1.凡前項費用未列之辦公事務費用屬之。 如文具用品、紙張、資料夾、郵資等。 2.單價未達 1 萬元或耐用年限未達 2 年
			小計	**409,953**	
三、設備及投資	電腦及周邊設備	30,000	4	120,000	電腦、網路交換器...等資訊設備(單價 1 萬元以上且耐用年限超過 2 年)，個人電腦/筆記型電腦*2(含作業系統及螢幕)單價上限 3 萬元、網路交換器*1。
			小計	**120,000**	
				1,902,990	

乙、人力規劃與工作執掌如下:

1. 計中主任：莊永裕 主任
2. 網路組組長：謝宏昀教授

3. 網路管理負責人：游子興

4. 資安業務負責人：李墨軒

5. 編制內及約聘僱專職人員：8 名

6. 協助處理各伺服器系統之例行維護、問題諮詢及統計監控使用狀況，Linux 伺服器系統維護、管理及統計使用者使用行為。撰寫網路管理應用相關文件，網路流量分析、監控及資料庫建立等。

五、基礎資料(網路管理及資安管理)

請依下列項目提供本年度報告資料

(一)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
(1)下游連線學校或連線單位數統計	連線學校(單位)數		1	31	13	1	5	連線單位總數：51
	連線單位比例		2%	61%	25%	2%	10%	註：單位數 / 總數
(2)連線頻寬與電路數統計	專線(非光纖)							
	光纖	10M(不含)以下						
		10M(含)以上 100M(不含)以下						
		100M(含)以上 500M(不含)以下						
		500M(含)以上 1G(不含)以下						
		1G(含)以上 10G(不含)以下		28	13	1	5	
		10G(含)以上	1	3				
	其他(如 ADSL 等)							
	連線電路小計		1	31	13	1	5	51
	連線頻寬合計(電路實際租用頻寬加總)		40G	58G	13G	1G	5G	連線頻寬總計：117

	連線頻寬比率	34%	49%	11%	1%	4%	請加總電路實際租用頻寬/總計頻寬

	縣(市)教育網路中心		連線頻寬		合計
(3)連線縣(市)教育網路中心	1.	____臺北市__教育網路中心	連線頻寬(亞太)	ipv4 + ipv6:20G	40G
			連線頻寬(中華)	ipv4 + ipv6:20G	
	2.	_____教育網路中心	連線頻寬(亞太)		
			連線頻寬(中華)		
	3.	_____教育網路中心	連線頻寬(亞太)		
			連線頻寬(中華)		

	連線單位名稱		連線頻寬	備註
(4)非學校之連線單位(不含 ISP)	1.	新北市立圖書館	1G	
	2.	中華民國高級中等學校體育總會	1G	
	3.	財團法人大學入學考試中心	1G	
	4.	中華民國學生棒球運動聯盟	1G	
	5.	國家地震中心	1G	
	6.			
	7.			
	8.			
	9.			
	10.			

		主節點名稱	連線頻寬	備註
(5)連線 TANet	1.	臺北主節點	100G	
	2.	新竹主節點	100G	

	ISP 名稱(AS)		連線電路數	連線頻寬(合計)	備註
(6)其他線路	1.	中華電信 Hinet(AS3456)	1	10Gbps	
	2.	新世紀資通 Seednet(AS4780)	2	2Gbps	
	3.	新世紀資通 NCIC(AS9919)			
	4.	中嘉和網 KBT(AS9461)	1	1Gbps	
	5.	台灣固網 TFN(AS9964)	2	2Gbps	
	6.	亞太電信 APG(AS17709)	1	1Gbps	
	7.	GGC server	2	20Gbps	
	8.				
	9.				
	10.				

(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

(二)區域網路中心資訊安全環境整備表

(1)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。 (請向教育部資科司資安窗口取得數據)	1.資安責任等級：B（核定日期：）。 2. 1、2級資安事件處理： (1)通報平均時數：0.001小時。 (2)應變處理平均時數：0.086小時。 (3)事件處理平均時數：0.087小時。 (4)通報完成率：100%。 (5)事件完成率：94.48%。 3. 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：0.003小時。

(2) 區域網路中心配合本部資安政策。 (請向教育部資科司資安窗口取得數據)	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：56.52 %。 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? V 是 □否 (2)是否符合稽核要求? V 是 □否 (3)符合資安專業證照人數：2 員 (4)維護之主要網站進行安全弱點檢測比率：100 %。

(三)區域網路中心維運事項辦理情形及目標

項目	111 年辦理情形	112 年目標
(1) 召開區管理會之辦理情形及成果(含連線單位出席率、會議召開次數) 。	6/30 第一次區網會議 出席率:94% (線上會議) 預計於 12 月舉辦第二次會議	預計於 6 月、12 月各舉辦一次 出席率: 90% 以上
(2) 骨幹基礎環境之妥善率。	99.99% 1.無骨幹斷線事件 2,僅有市網遭受 DDoS 攻擊時，骨幹 BGP 因 BFD up/down 頻繁切換造成使用者 Session 中斷，合計應不超過 1 小時。	目標: 99.9%
(3)連線學校之網路妥善率。	連線學校網路中斷可能原因:1.計畫性維修. 2.ISP 電路異常斷線. 3.連線單位設備異常斷線. 因本年度未詳細統計連線學校斷線原因，因此無法提供此數字。	目標:99 % 詳細統計連線學校斷線原因
(4)辦理相關人員之專業技術推廣訓練。	暑期課程:11 門(線上)	暑期課程:10 門

	每堂課參與人數: 100 人以上	實做課程: 50% 每堂課參與人數: 40 人 (因電腦教室限制)
(5)連線學校之 IPv4/IPv6 推動完成率。	大專院校: 94% 高中以下及其他單位: 80%	大專院校: 100% 高中以下及其他單位: 90%
(6)協助連線學校之網管及資安工作。 ●建立區網路維運管理機制。 ●協助連線學校網路的維運或障礙排除(含諮詢) 。 ●建立資安防護或弱掃服務(含諮詢)。 ●建立連線學校相關人員聯繫管道及聯絡名冊。	2022/05/09 : ASR 與 Gigamon 40G 擴增至 80G 2022/06/02 : 市網 20G 擴增至 40G 2022/10/12 : 台固 1G 擴增至 2G 因表格有限，其他項目詳列於貳、參項。	區網課程上機實做課程: 佔 50%以上 技術文件分享: 完成 3 份以上網路資安文件撰寫 推廣無線漫遊認證: 建置於 2 個單位以上 推廣網路品質監控系統: 建置於 3 個單位以上
(7)服務滿意度。	整體服務滿意度: 88.6%	整體服務滿意度: 90%
(8)其他:(各區網自行新增欄位)		

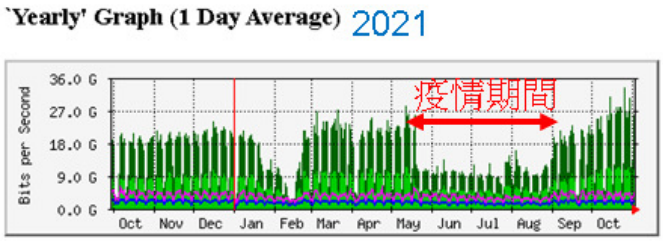
貳、請詳述貴區網中心之網路連線、網管策略及具體辦理事項(網路管理)

說明:1.111 年度網路管理維運具體辦理事項。

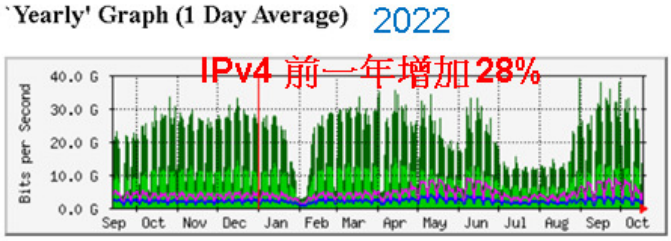
2.112 年度網路管理營運方針。

甲、111 年網路流量使用狀況:

IPv4 流量

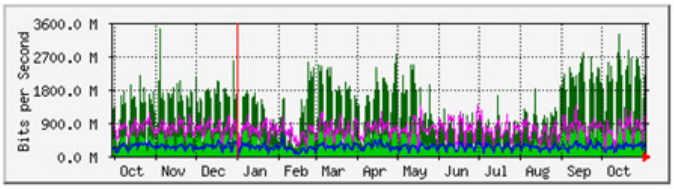


	Max	Average	Current
台北主節點 => 北區區網	33.2 Gb/s (33.2%)	6115.1 Mb/s (6.1%)	10.8 Gb/s (10.8%)
北區區網 => 台北主節點	6075.9 Mb/s (6.1%)	1676.6 Mb/s (1.7%)	1825.1 Mb/s (1.8%)

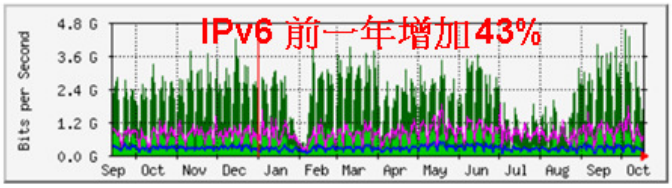


	Max	Average	Current
台北主節點 => 北區區網	39.0 Gb/s (39.0%)	7882.8 Mb/s (7.9%)	11.7 Gb/s (11.7%)
北區區網 => 台北主節點	8786.5 Mb/s (8.8%)	1862.4 Mb/s (1.9%)	2506.5 Mb/s (2.5%)

IPv6 流量



	Max	Average	Current
台北主節點 => 北區區網	3431.8 Mb/s (3.4%)	372.0 Mb/s (0.4%)	732.0 Mb/s (0.7%)
北區區網 => 台北主節點	1361.6 Mb/s (1.4%)	232.1 Mb/s (0.2%)	270.7 Mb/s (0.3%)



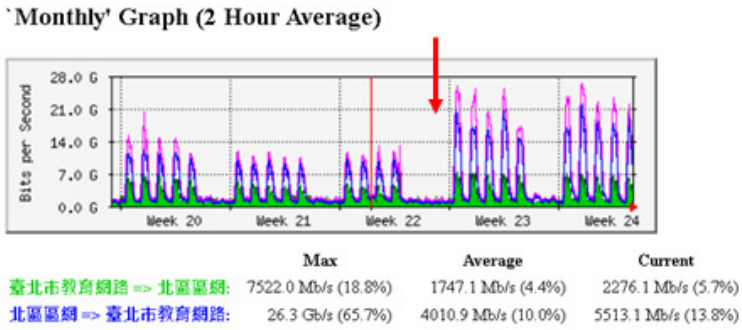
	Max	Average	Current
台北主節點 => 北區區網	4541.2 Mb/s (4.5%)	533.3 Mb/s (0.5%)	785.2 Mb/s (0.8%)
北區區網 => 台北主節點	1804.7 Mb/s (1.8%)	233.6 Mb/s (0.2%)	243.3 Mb/s (0.2%)

乙、111 年區網骨幹網路電路異動資訊:

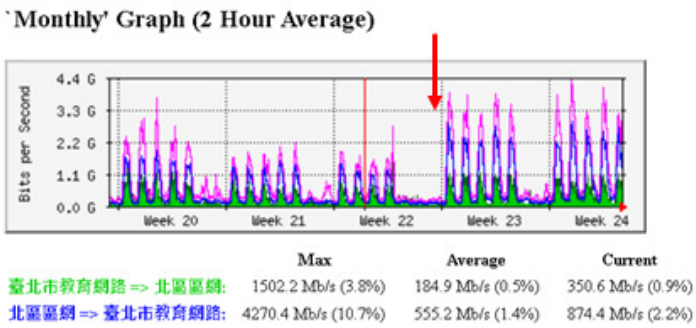
2022/05/09 : ASR 與 Gigamon 40G 擴增至 80G
2022/06/02 : 市網 20G 擴增至 40G
2022/10/12 : 台固 1G 擴增至 2G

丙、臺北市網線路 20G 擴增至 40Gbps: 流量變化

* 臺北市網 ipv4



* 臺北市網 ipv6

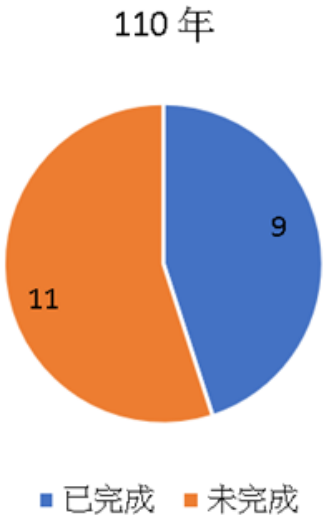


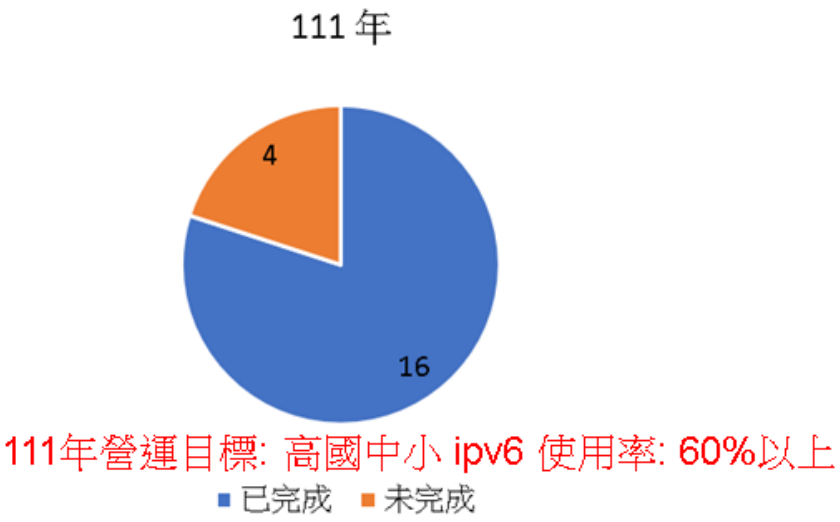
丁、IPv6 連線單位完成率統計

大專院校: 31 間

有 ipv6 網段學校全部完成
尚無 ipv6 網段:軍事情報局學校、臺北基督學院

高國中小及其他單位: 20 個

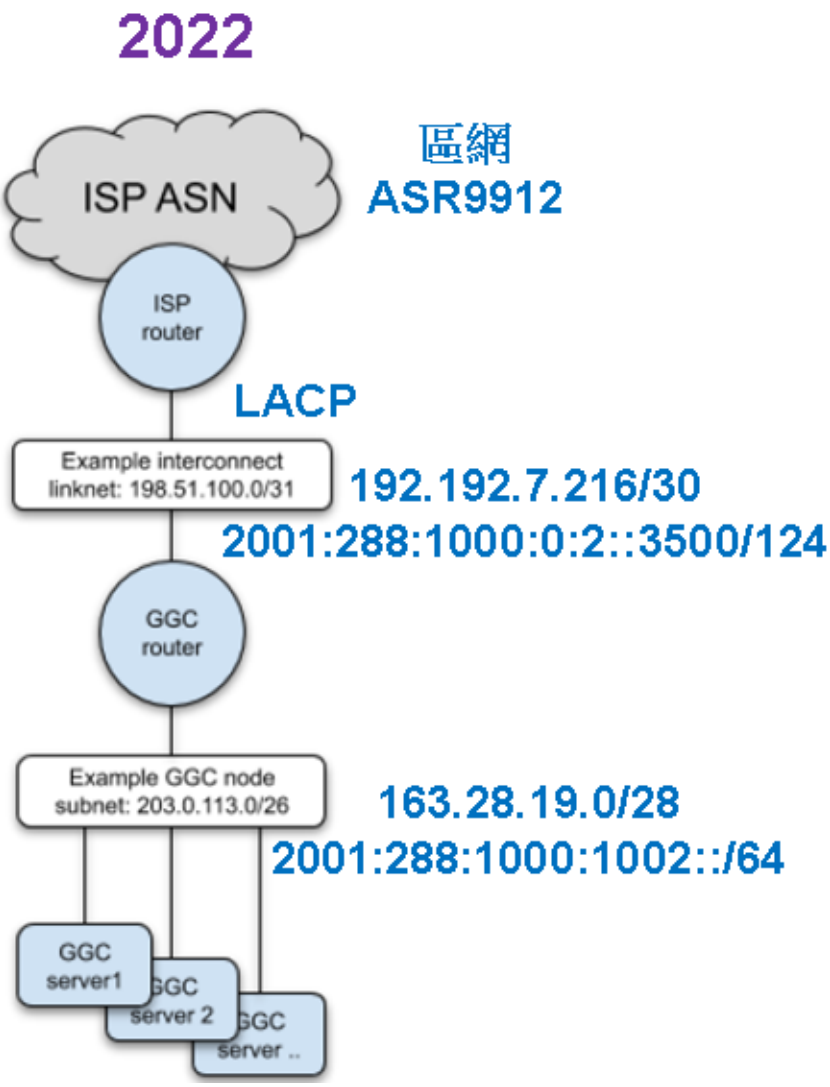




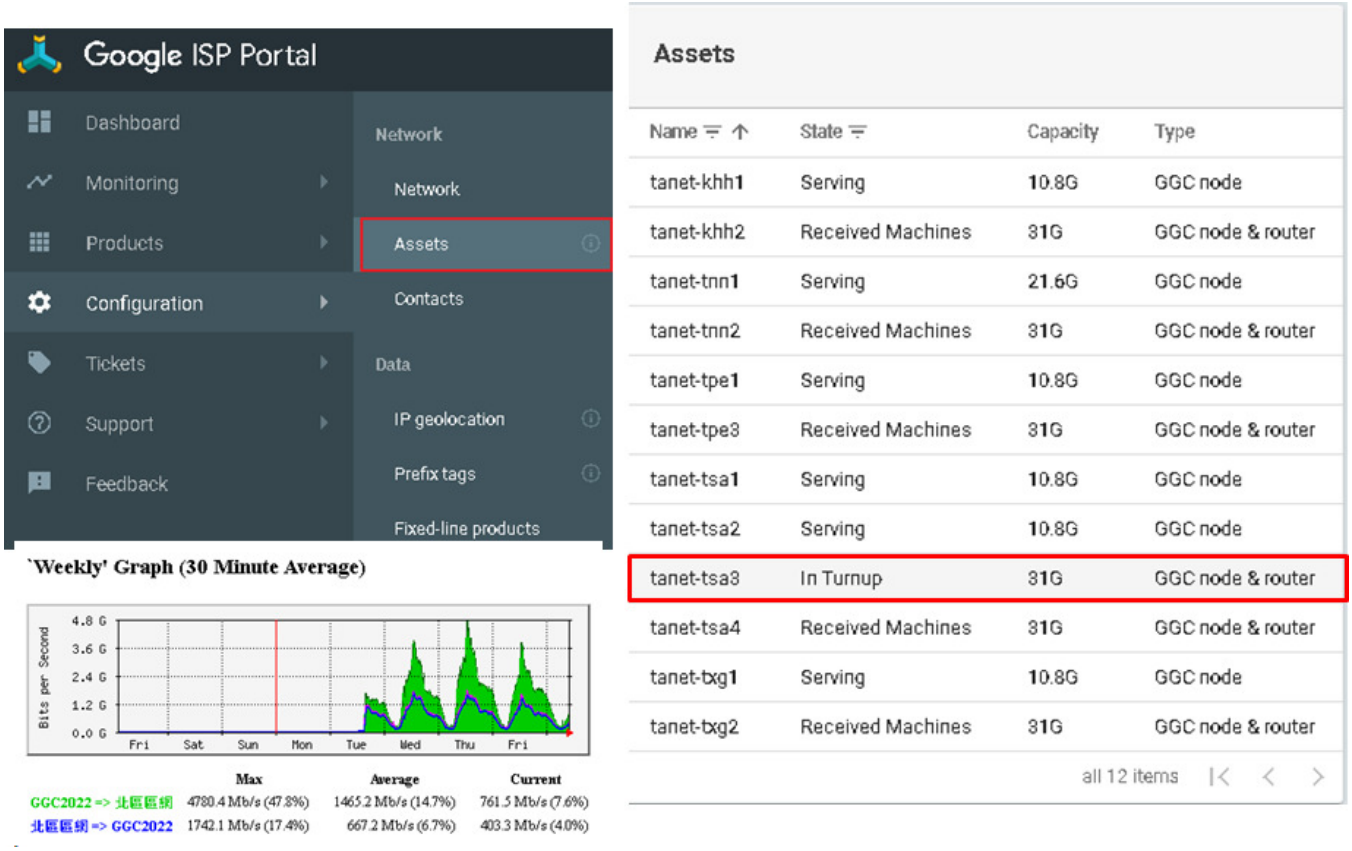
111年營運目標: 高國中小 ipv6 使用率: 60%以上

有 ipv6 網段學校全部完成
尚無 ipv6 網段:大學入學考試中心、中華民國學生棒球運動聯盟、高中體育總會、國家地震中心

戊、Google Global Cache 2022 建置完成架構圖



2022/08/29 TurnUp 上線: 臺北區網 1 是第一個將 GGC 2022 上線之區網中心因設定架構與舊 GGC 架構不同，提供 ASR 設定指令供其他區網中心參考。



2022/09/03 OLD GGC 下線: 新舊 BGP Session 切換記錄

- #sh bgp ipv4 unicast summary

Old BGP

New BGP

```
Neighbor        Spk    AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down  St/PfxRcd
139.175.59.145    1  4780 1951836 1771766   831900    0    0    19w2d       3032
139.175.59.149    1  4780 1952262 1772181   831900    0    0     3w1d       3032
140.112.0.69      1 17716  885612  984854   831900    0    0    1y35w          4
163.28.18.16      1 65535 1771194 1780801        0    0    0 01:19:10 Active
192.192.7.106     1 18183 1930279 1772072   831900    0    0    1y30w          4
192.192.7.218     1 36040    5792    5928   831900    0    0    3d21h          1
192.192.61.82     1  1659 173606676  885178   831900    0    0     6w0d          1
192.192.61.86     1  1659 200407782  884947   831900    0    0    17w3d          1
203.79.255.205    1 17709 1881276 1772279   831900    0    0     2w4d       1435
203.133.92.65     1  9416  901662  886385   831900    0    0    1y35w        206
211.78.221.25     1  9924 2484827 1771814   831900    0    0    4d11h       1532
220.128.33.18     1  3462 2116528 1772110   831900    0    0    1y02w       2346
```

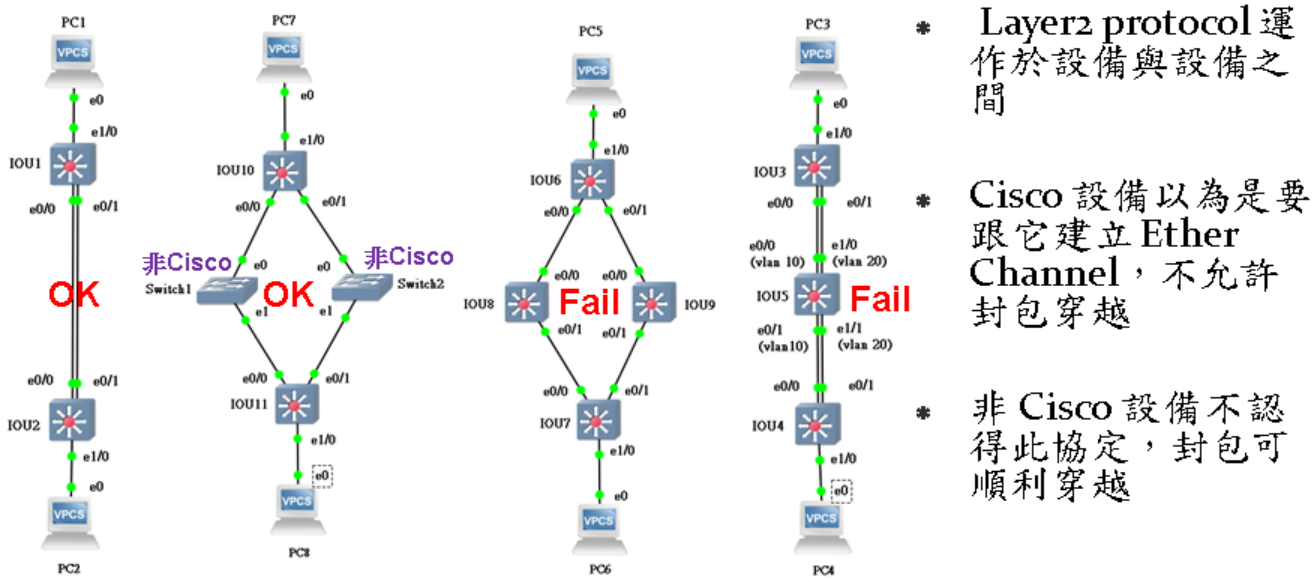
- #sh bgp ipv6 unicast summary

New BGP

Old BGP

```
Neighbor        Spk    AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down  St/PfxRcd
2001:288:0:1659:192:192:61:81
                  1  1659 211887585  883485     9262    0    0     6w0d          1
2001:288:0:1659:192:192:61:85
                  1  1659 263216070  883710     9262    0    0    17w3d          1
2001:288:1000:0:2::3502
                  1 36040    5790    5790     9262    0    0    4d00h          1
2001:288:1000:1001::10
                  1 65535 1771179 1771370        0    0    0 01:19:18 Idle
2404:0:10ff:1:7709:1:7716:0
                  1 17709 1868782 1771109     9262    0    0    11w6d        104
```

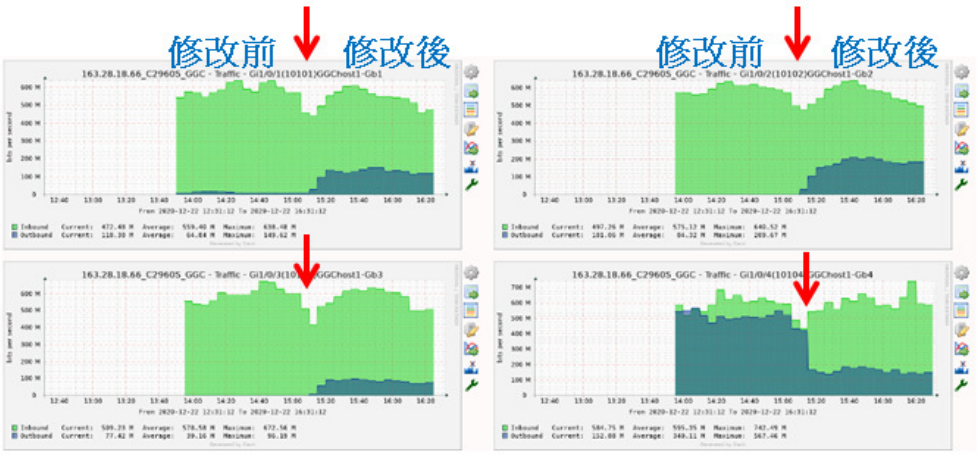
己、租用點對點電路是否支援 LACP/Ether Channel ?



結論: 若租用之點對點電路中間未使用具網管功能可辨識 LACP 協定之設備，則可支援甲乙端使用 LACP/Ether Channel 協定。

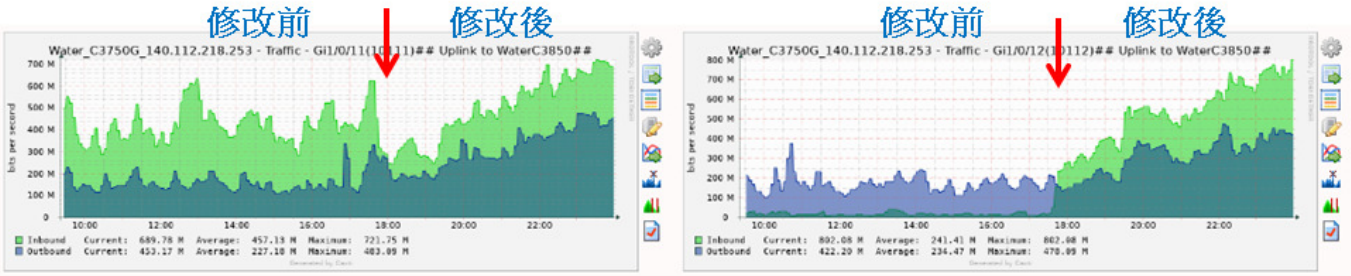
庚、LACP Load Balance 預設演算法可能造成流量不平均

* 預設演算法: src-mac，造成流量不均
  * C2960 To GGC Server 1(1G x4)



* 建議改成 src-dst-ip，Src XOR Dst IP Addr

* 預設演算法: src-mac，造成流量不均
  * 水源校區 2G x 2



* 改成演算法: src-dst-ip，流量平均

辛、無線漫遊推廣與建置

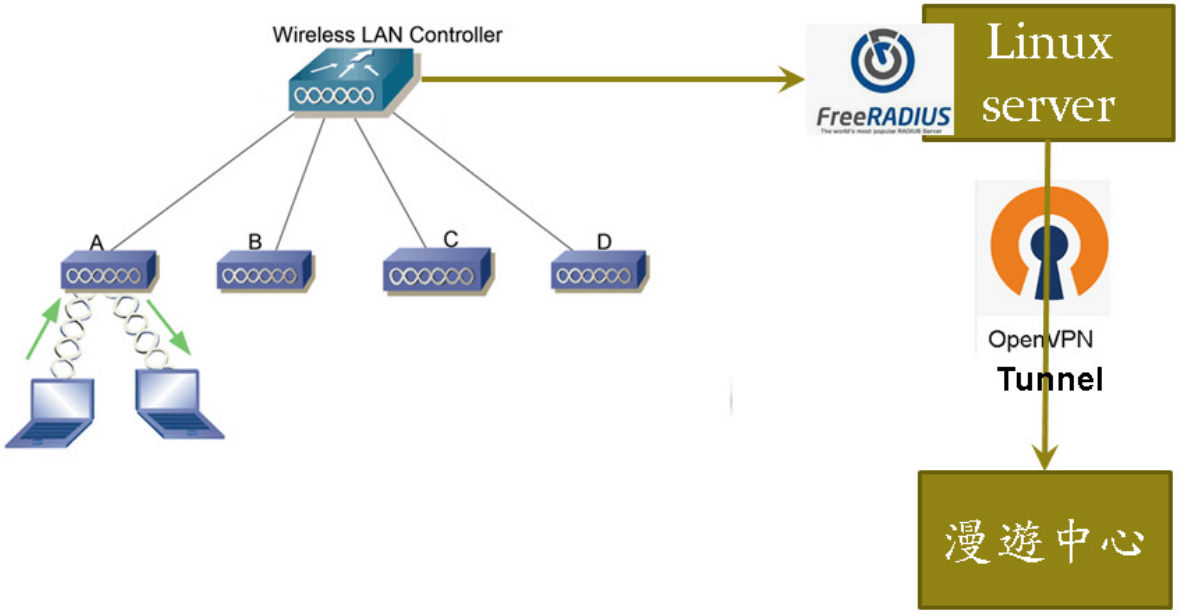
1.於第一次區網會議，請漫遊中心分享：TANet 無線漫遊建置與維運

2.協助”樹人家商”建置無線漫遊

i.撰寫 Ubuntu 安裝設定手冊:(漫遊中心原僅有 CentOS 安裝手冊)

ii.OpenVPN, FreeRadius 設定

* 自行繪製架構圖供連線單位參考



壬、112 年度網路管理營運方針

1. 網路妥適率: 99.9%以上

2. 區網網管會議出席率: 90%以上

3. 大專院校 ipv6 使用率: 100%

4. 高國中小 ipv6 使用率: 80%以上

5. 區網課程上機實做課程: 佔 50%以上

6. 推廣無線漫遊認證: 建置於 2 個單位以上

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)

說明:1.111 年度資安服務維運具體辦理事項。
2.112 年度資安服務目標(實施措施)。

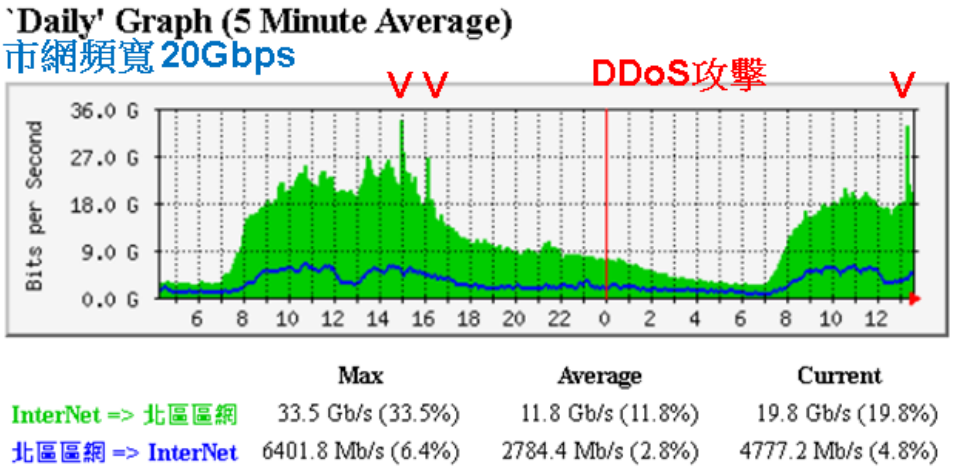
甲、108~111 年度資安事件統計

	108	109	110	111
1、2級資安事件處理				
通報平均時數	0.586 小時	0.04 小時	0.05 小時	0.001 小時
應變處理平均時數	0.017 小時	0.05 小時	0.86 小時	0.086 小時
事件處理平均時數	0.602 小時	0.74 小時	1.42 小時	0.087 小時
通報完成率	99.969%	100 %	99.89 %	100 %
事件完成率	99.627%	100%	100%	94.48%
3、4級資安事件通報	無	無	無	無
資安事件通報審核平均時數	0.206小時	1.12小時	0.55小時	0.003小時
資料更新完整校數	81.633%	97.04%	100%	56.52%

乙、2022/04、05 市網 DDoS 攻擊事件

1. 攻擊發生時間及流量

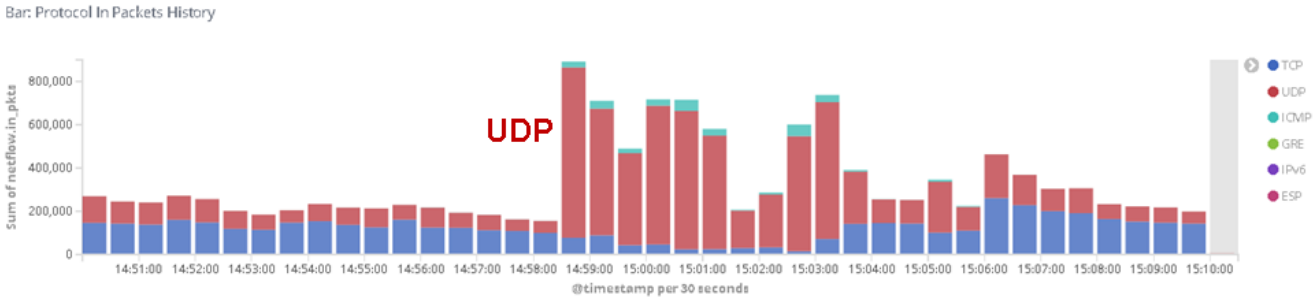
* 2022/04/01 14:00~14:30
* 2022/04/28 15:00~15:05
* 2022/05/09 09:30 10:00 14:00 2022/05/10 09:50
* 2022/05/13 14:20 17:00



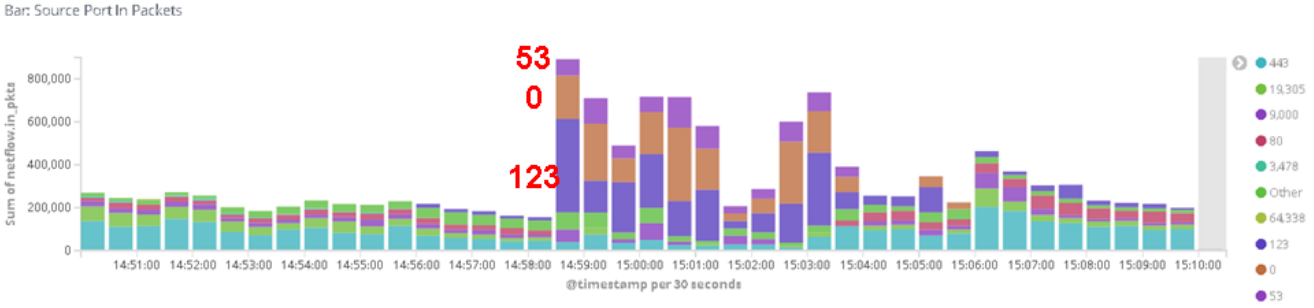
	Max	Average	Current
InterNet => 北區區網	33.5 Gb/s (33.5%)	11.8 Gb/s (11.8%)	19.8 Gb/s (19.8%)
北區區網 => InterNet	6401.8 Mb/s (6.4%)	2784.4 Mb/s (2.8%)	4777.2 Mb/s (4.8%)

2. 攻擊來源分析

* Protocol: UDP

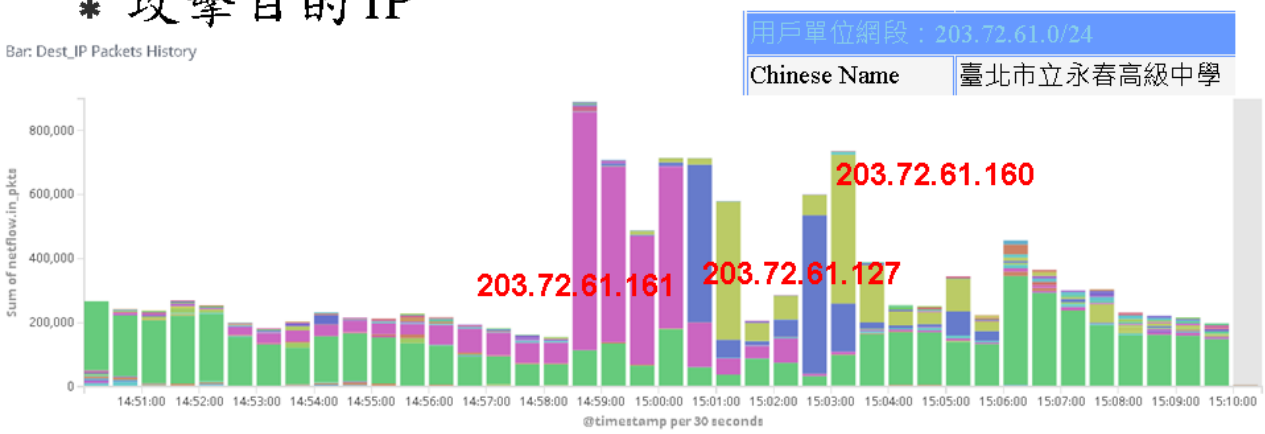


* Source Port: DNS, NTP 放大攻擊



3. 攻擊來源分析

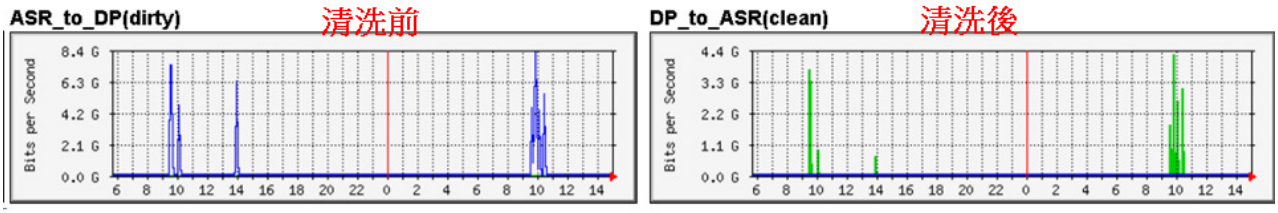
* 攻擊目的 IP



* 每次不盡相同

4. DDoS 攻擊緩解方法

* 北區 ASOC 流量清洗



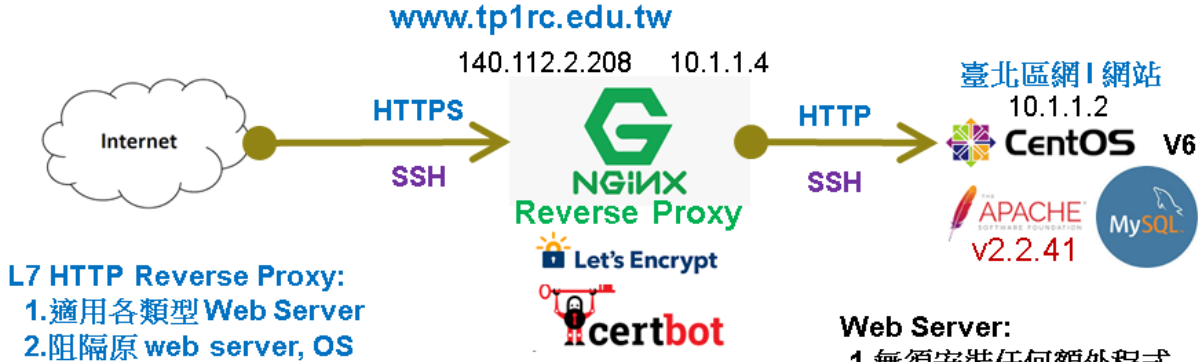
* ASR 至 Gigamon 分流器頻寬: 40G 擴增至 80G
* 暫時移除 ASR 與主節點 BGP 之 BFD 設定

丙、區網網頁新架構

網頁攻擊事件:

- 2022/08/02 美國國會議員裴洛西訪台
- 遭受網軍進行網頁置換攻擊
- 區網首頁潛在風險
  - PHP + MySQL: 歷史悠久、歷代更迭
  - 動態網頁：公佈欄、連線單位資訊資料庫
  - 網頁後台管理系統
- 解決方案
  - 純靜態網頁: 無後台管理功能、無動態程式功能
  - 公版網頁範本
  - 商用WAF:經費有限

區網網頁新架構:

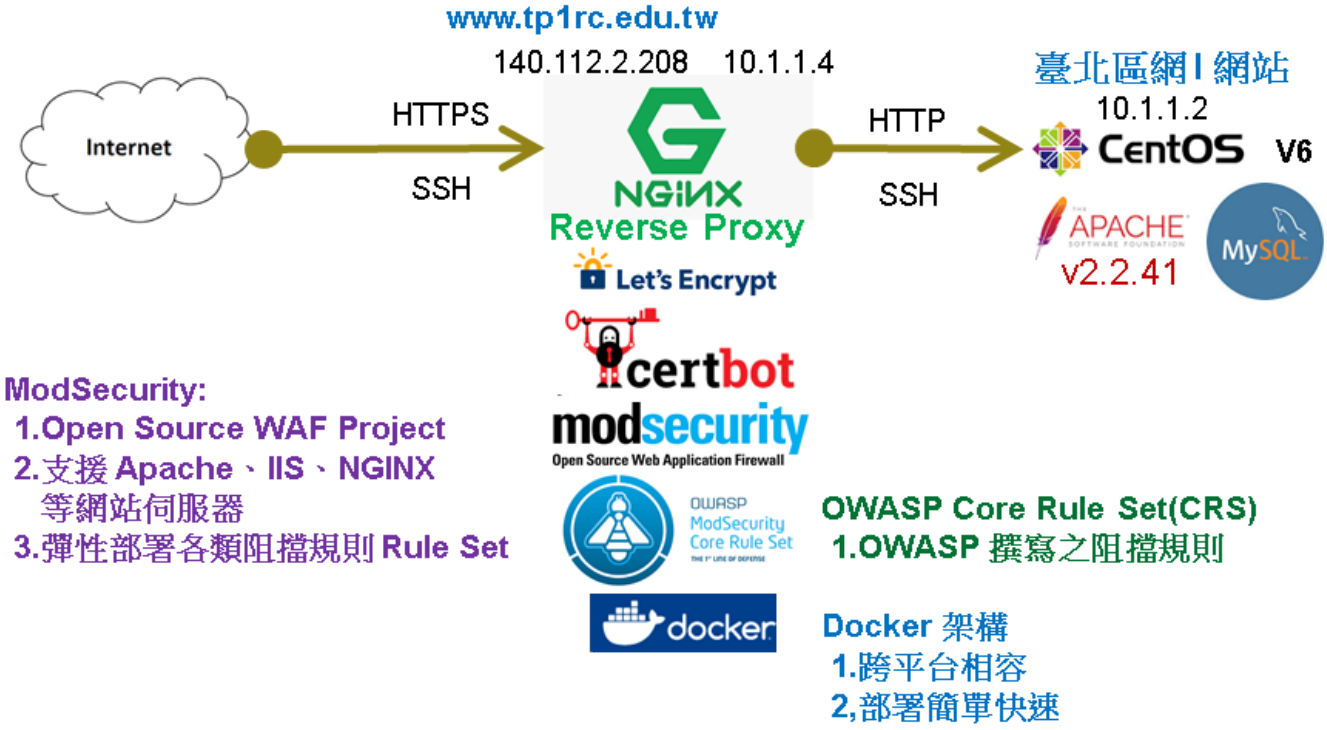


L7 HTTP Reverse Proxy:
1.適用各類型Web Server
2.阻隔原 web server, OS 暴露於 Internet.
3.額外提供 Load Balance、Content Cache、WAF 功能.

L4 SSH Reverse Proxy:
1. SSH 遠端登入
2. sftp 異地備份

Let's Encrypt 免費憑證：
1.Certbot 安裝於NGINX，不影響原 Web Server
2.憑證到期自動 Renew
3.減輕後端 Web Server SSL/TLS 加解密 Loading
4.後端非加密封包可額外安裝 IDS/IPS

Web Server:
1.無須安裝任何額外程式
2.原 MRTG 服務(需內對外連線)，移至別台機器.
3.改用虛擬IP，移除 Gateway IP 設定
※避免未知後門/木馬(如:Reverse Shell)
持續運作.



區網網頁入侵測試:

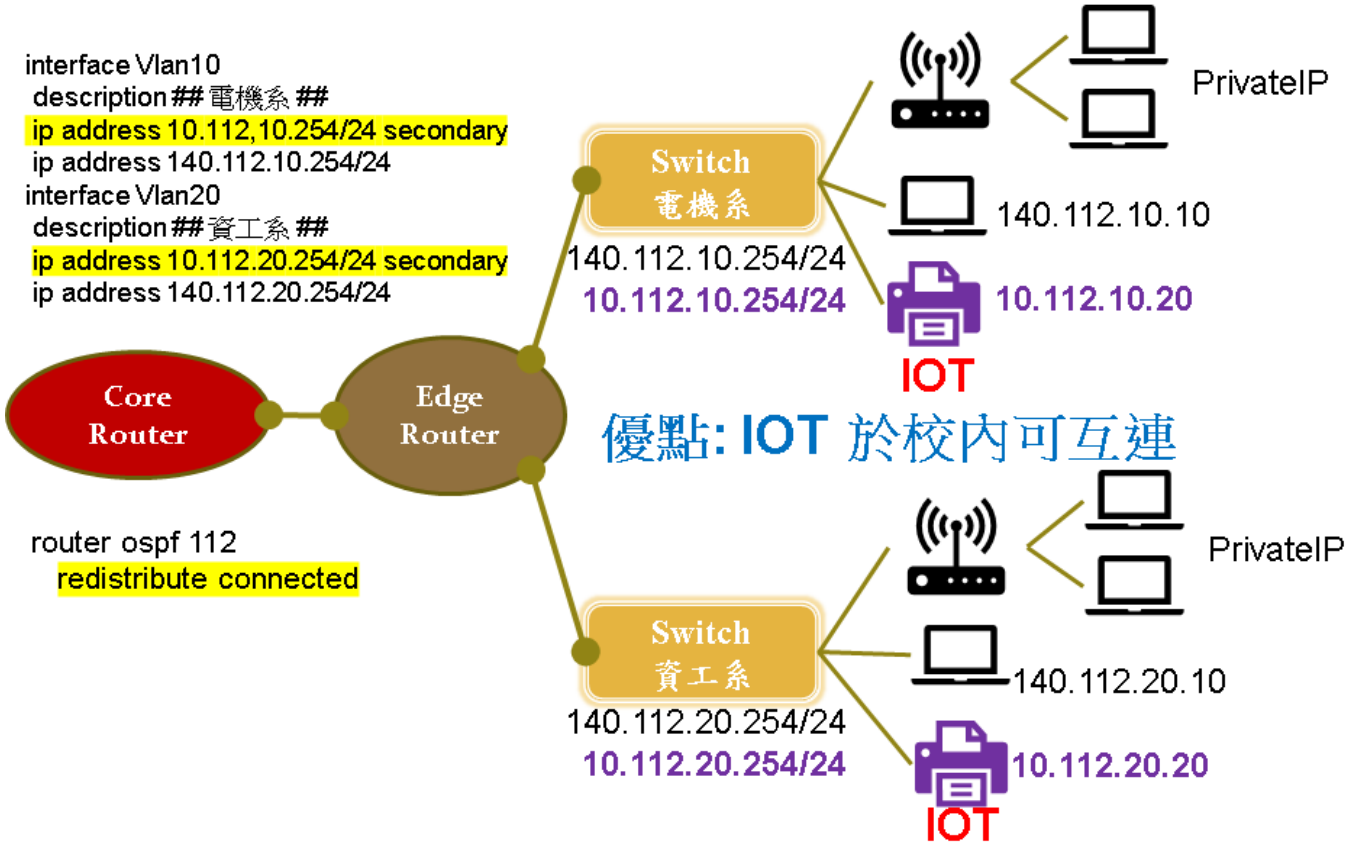
* **Command Injection 測試**
  * https://www.tp1rc.edu.tw/index.php?a=/bin/sh
* **SQL Injection、XSS 測試**
  * 連線單位登入系統
  * 管理後台

  * SQL Injection:' or 1=1 --
  * XSS(Cross-Site Script): <script>alert(1)</script>
* **Web Shell 測試**
  * 一句話木馬(Simple Shell)
    * http://www.tp1rc.edu.tw/https/simple-shell.php?cmd=cat+/etc/passwd
  * B374K Shell
    * 可順利登入，但大部分功能無法運作
    * http://www.tp1rc.edu.tw/https/b374k.php

丁、物聯網設備之風險與控管

* 風險與危害
  * 資訊洩漏
  * 駭客內網跳板
  * DDoS 幫兇
  * 加密與勒索
  * 資源浪費
    * 挖礦: 電力
    * 印表機勒索:紙張
* 解決方法
  * OS、韌體定時更新
  * ACL 設定
  * 避免暴露於 Internet

物聯網: 避免暴露於 Internet，校內路由器開通互連虛擬 IP 網段



戊、111 年度區網課程(11 門)

分類	日期	講題	講者	報名
網路	8/15	Google Workspace for Education 與 Google Meet 實用技能運用 (含 Demo)	CloudMile 吳鳳元 Franky Wu	**154**
資安	8/16	運用零信任策略落實身份治理與單一簽入整合	鋐迪資訊股份有限公司 Andy Chung 鍾迪 資深技術顧問	**90**
程式	8/19	無痛連結 Google Workspace, REST APIs (含 Demo	CloudMile 陳伯維 Martin Chen	**125**
資安	8/22	從資安到 AI，掌握 Google 全方位雲端生態 (含 D	CloudMile 吳鳳元 Franky Wu	**102**
法規	8/24	校園智財權--著作權授權合約之實務運作	胡中瑋律師	**99**
法規	8/25	ISO 27002 : 2022 資訊安全實務指導規範之新版本	資誠聯合會計師事務所 經理	**140**
網路	8/30	開源網路設備監測系統	中央大學電算中心許時準	**139**
網路	8/31	疫情期間居家辦公 VPN 自動化管理、電子郵件攻 探討	臺北藝術大學電算中心 長	**126**
程式	9/13	無痛連結 Google Workspace, REST APIs (含實作) （進階）	CloudMile 陳伯維 Martin Chen	**125**
網路	9/20	Google Workspace for Education 與 系統管理/雲端安全工作術 (含 Demo)	CloudMile 吳鳳元 Franky Wu	**117**
網路	9/27	Google Classroom 實際場景應用，打造高效線上	CloudMile 吳鳳元 Franky Wu	**52**

己、111 年度資安服務維運具體辦理事項

1. ASOC 資安警訊通報，協助通報連線學校，並提供技術支援。
2. 配合資安關懷，協助解決未能解決的資安事件。
3. 協助追蹤重大資安事件。
4. DDoS 清洗申請及通報。
5. 與 ASOC 合作，有重大資安警訊時通知 ASOC，ASOC 協助找出學網內可能有資安警訊之設備。區網再通知連線學校處理。
   (1) 10 月網路攝影機預設帳密事件
   (2) 9 月 FTP 暱名登入
   (3) 8 月 XOOPS CMS 網站內容管理系統發現嚴重資安漏洞
   (4) 7 月 QNAP 遭到駭客組織「Checkmate」鎖定進行勒索軟體攻擊
   (5) 5 月 F5 BIG-IP 漏洞
   (6) 1 月 Windows 作業系統有遠端桌面(RDP)的漏洞

庚、112 年度資安服務目標(實施措施)

6. 區網網路與資安課程: 10 場以上
7. 區網課程上機實做課程: 佔 50%以上
8. 技術文件分享: 完成 3 份以上網路資安文件撰寫

9.推廣網路品質監控系統: 建置於 3 個單位以上

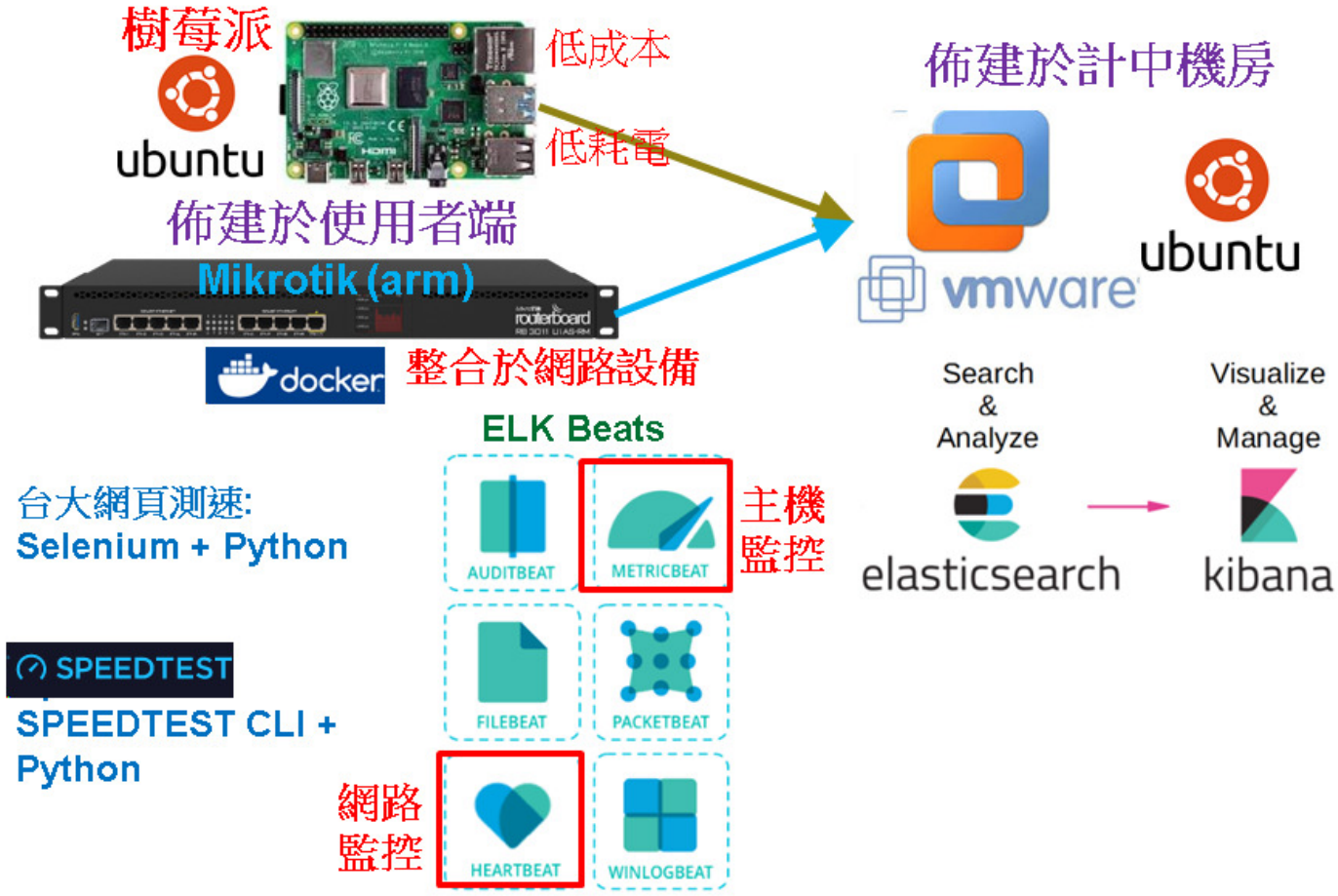
肆、特色服務

一、請說明貴區網中心服務推動特色、辦理成效。

說明:1.111 年度服務特色辦理成效。

2.其他專案服務(教育部或其他機關補助或計畫專案之服務規劃或成果,無則免填)。

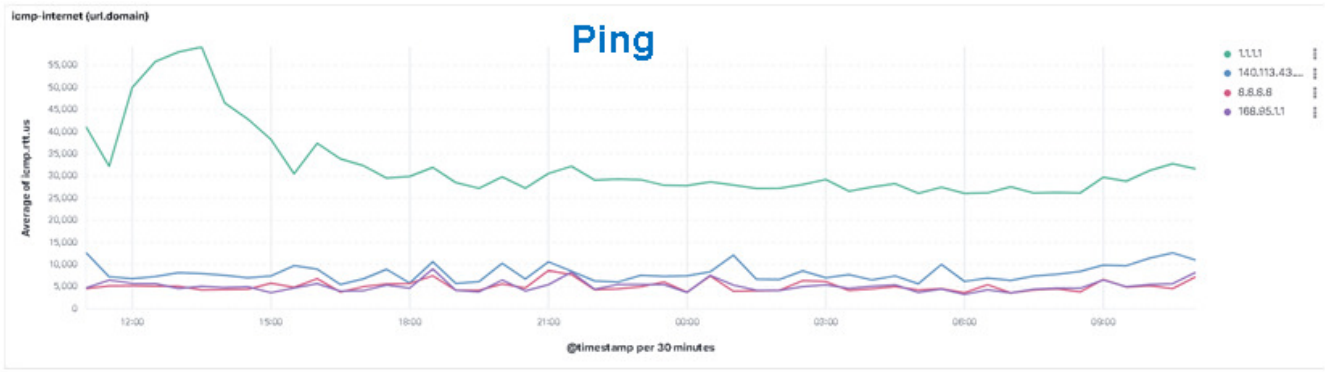
甲、使用者端網路品質監控系統

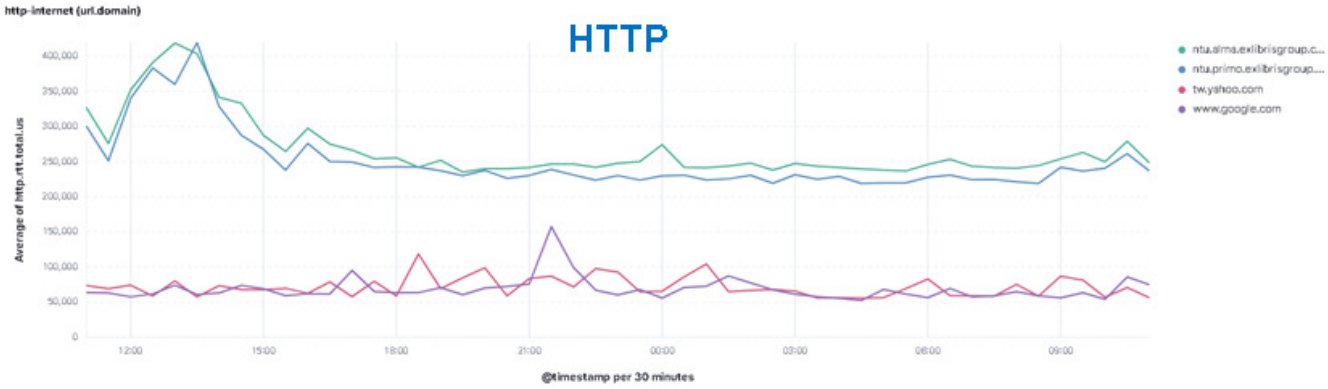


乙、網路測速

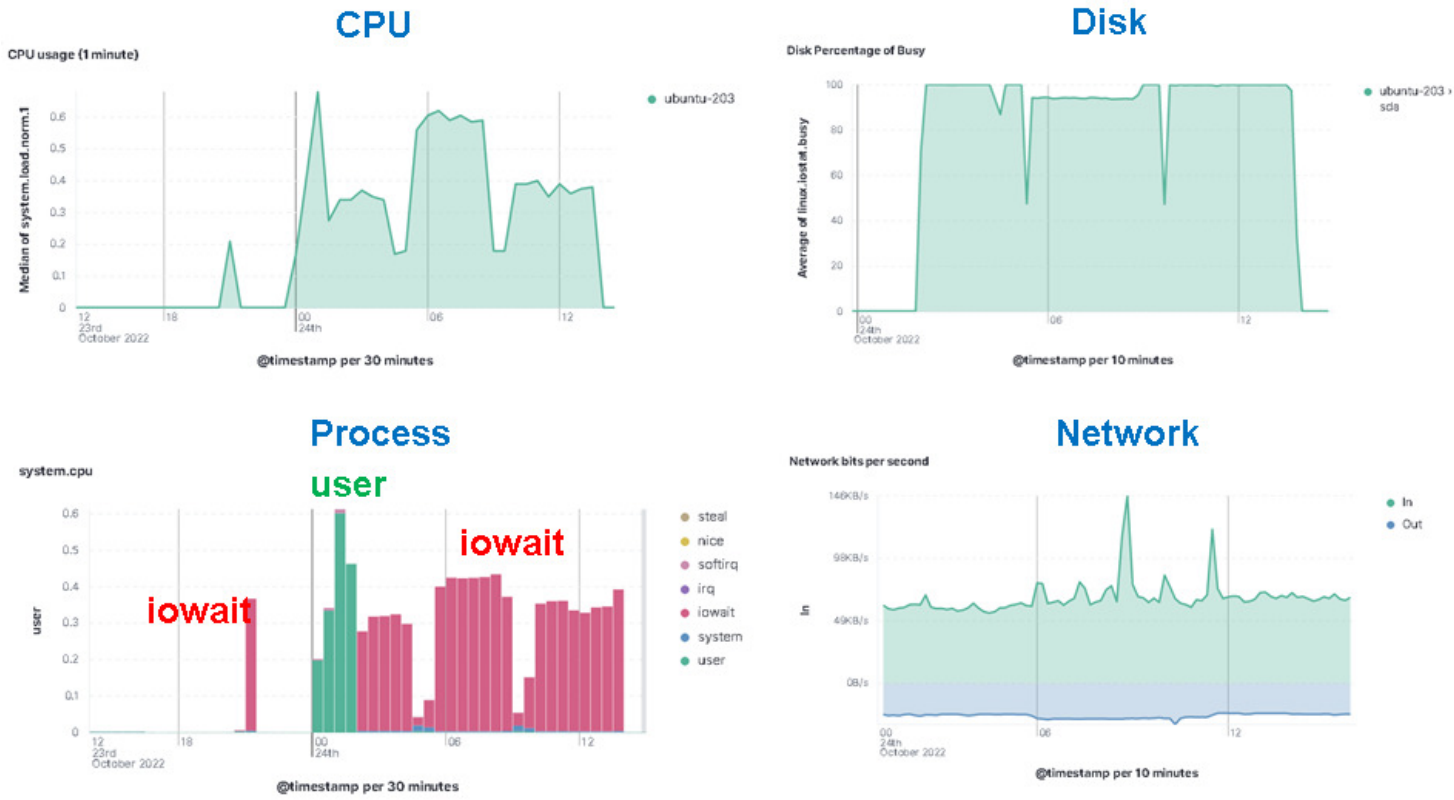
* speedtest http://www. speedtest.net
* 台大測速 http://speed5.ntu.edu.tw/

丙、ELK Heartbeat 網路監控

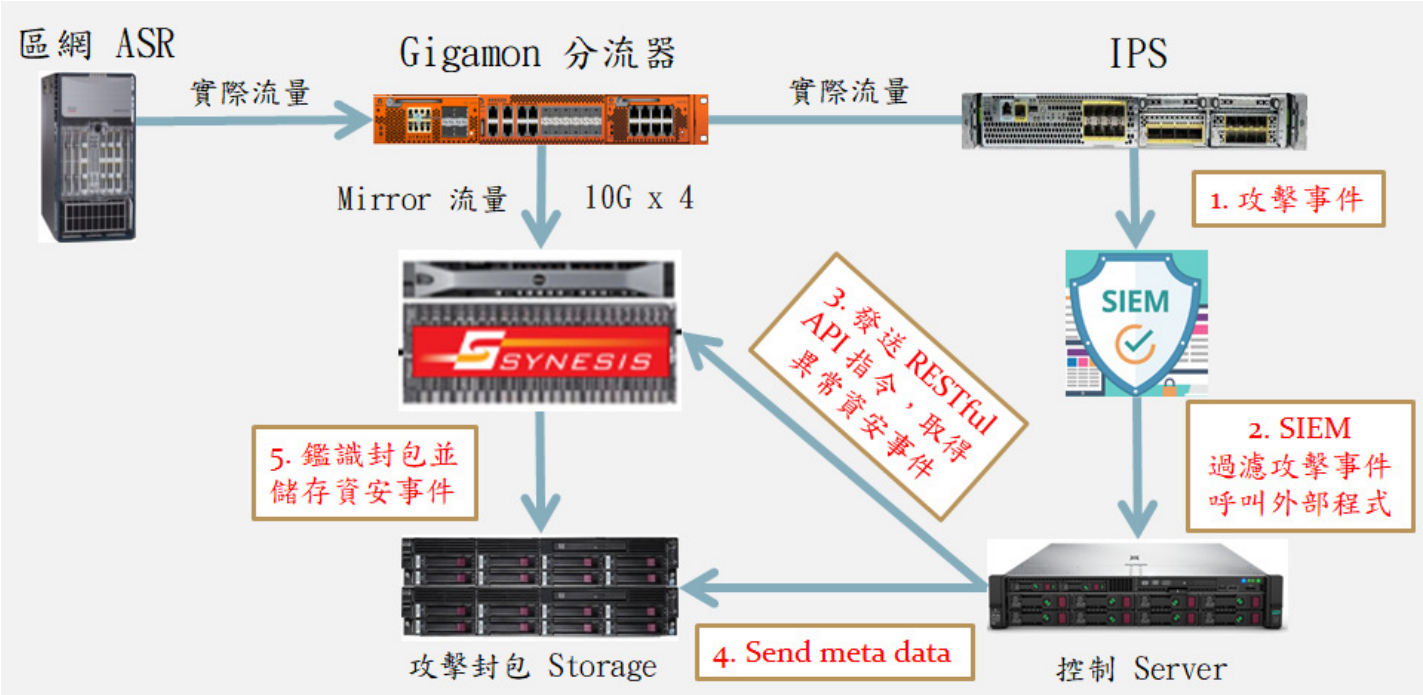




丁、ELK Metricbeat 主機監控



戊、實習場域計畫:與北區 A-SOC 合作計畫



●預期效益:

1. 資安事件封包分析、降低誤判率:

(1) IPS 設備僅能保留觸發事件規則之唯一封包

(2) 若有完整事件封包檔，可進一步分析觸發主機資訊: OS Fingerprint、HTTP Agent、Web Server App/Version、加密憑證資訊.

(3) 降低誤報率: 例. Apache 事件單不應開給 Windows IIS 伺服器

2. 豐富開單訊息: 挖礦事件為例:

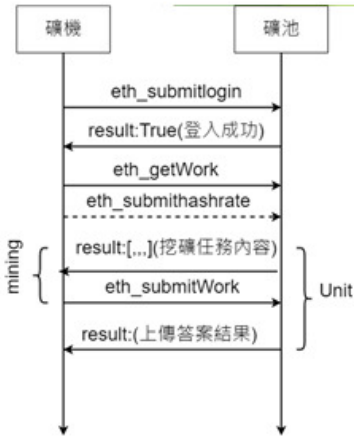
原事件單

事件主旨	教育部資安通告-國立[redacted]大學[120.[redacted]]主機疑似進行挖礦程式連線(PUA-OTHER Cryptocurrency Miner outbound connection attempt)
事件描述	入侵偵測防禦系統偵測到來源IP（120.[redacted]），包含疑似挖礦程式連線行為，對目標IP（1[redacted]進行連線。此事件來源 PORT（53857），目標 PORT（3333）。
手法研判	來源IP可能遭入侵並對外部虛擬貨幣挖礦伺服器報到進行挖礦行為，故依教育部資安政策，進行開單告警。

豐富資訊

入侵偵測防禦系統偵測到來源IP（120.x.x.x），疑似進行以太幣挖礦行為使用ethminer程式並使用Stratum協議與礦池進行要工作的(mining.subscribe)連線行為，錢包地址為 0x4296116d44a4a7259B52B1A756e1，挖礦程式的hashrate為_YY_，有挖礦成功記錄(___Nonce值)，礦池IP（139.162.81.90）進行連線。此事件來源 PORT（53,857），目標 PORT（3333）。

封包分析



3. Open Data 特色封包資料集

(1) I 建立去識別化之 DNS 放大攻擊封包資料集

(2) 已運用於 111 年台大資安課程實做 Lab: 辨識攻擊類型、計算放大倍率、辨識攻擊封包與反射封包.

二、未來創新服務目標與營運計畫。

說明:1.112 年度創新服務目標與構想。

2.創新特色議題對 TANet 網路或資安管理有助益之特色服務。

1.推廣 Open Source WAF 網頁防禦系統。

2.其他建議: TANet 網路品質測試系統

✱ 目前僅能提供當下測試結果

✱ 建議能查詢過去歷史記錄

✱ 主動定時測試(例如. 每五分鐘)，並提供歷史統計圖表

伍、前年度執行成效評量改進意見項目成效精進情形

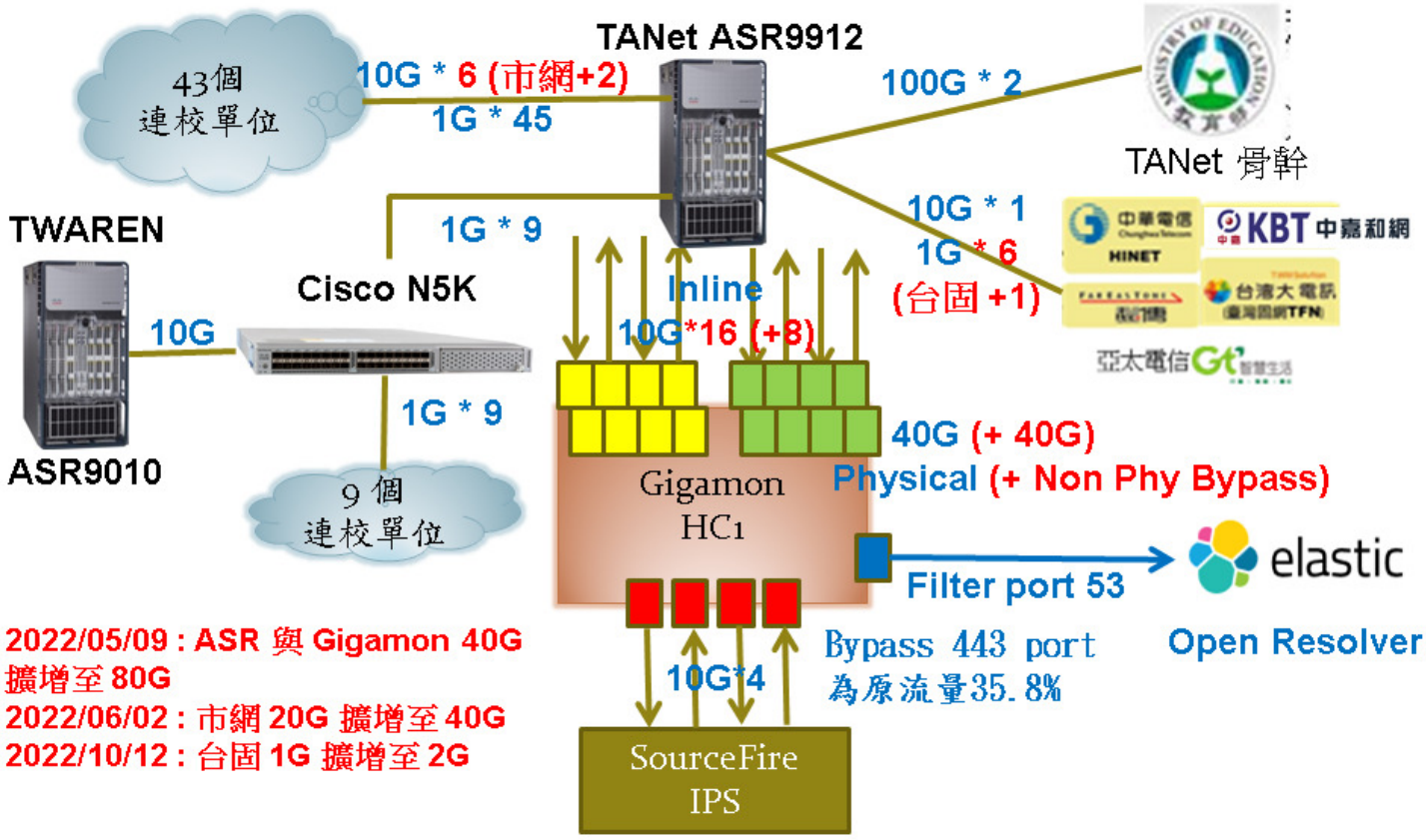
No	委員建議	回覆
1	報告中加強說明對連線單位之協助。	1.協助樹人家商無線漫遊建置。

		2.協助連線單位進行 DDoS 清洗與阻擋。 3.協助市網新增電路與擴頻。
2	資安、網路技術特色技術經驗之推動分享報告較為不足可持續加強。	1.區網會議、中山區網暑期課程分享 HTTPS 憑證原理與安裝及加密流量分析 2.受邀國教署教育部智慧網路環境提升計畫分享:網路設備採購規格及機房網路規劃
3	A-SOC 互動及經驗資料	共同參與實習場域計畫，計畫目標包含: (1)資安事件封包分析、降低誤判率(2)豐富開單訊息: 挖礦事件為例(3)Open Data 特色封包資料集
4	建議在書面成果報告中，可就區網中心整體或各單位網路使用概況作進一步分析，當可呈現使用使用趨勢及未來需求之推估 。	已更新於書面成果報告中。
5	建議將網路監控技術推廣至連線單位，當可就以發展之技術循環改善	1.於區網會議及校內網管會議分享佈建網路監控之相關技術及實際作法。 2.持續精進網路監控技術，今年增加使用 Elastic Stack metricbeats 套件,可監控主機與 ESXi VM 環境之效能。
6	建議可就網路管理維運所需技術定期更新整理，並將成果加以分享 。	1.於區網會議及校內網管會議分享佈建網路監控之相關技術及實際作法。 2.課程講義皆已公佈於區網網頁中。
7	應將 IPv6 及 eduroam 之推動納入區網中心維運目標，並設定質化及量化目標 。	1.協助樹人家商無線漫遊建置。 2.所有連線單位有配發 ipv6 之單位皆已完成 Peer IP 與路由設定。 3.明年度預計請尚未申請 IPv6 網段之單位儘速申請。
8	教育訓練課程應持續尋求數位化保存。	1.歷屆所有暑期課程講義皆已公佈於區網網頁中。 2.逐步整裡過去課程錄影資料，適當剪輯後公佈於區網網頁中。
9	網路妥善率以 99%為目標，以年度計算，可容許障礙時間為 88 小時，建議可再設法精進，其他指標也建議一併思考精進	1.訂定網路妥善率 99.9%以上。 2.配合 ISO27001 稽核要求，擬定各種異常斷線 BCP 演練計畫，可降低事故發生時之處理時間。
10	7/30 100G 骨幹斷線 1 小時 40 分，其原因為線路及卡版各一故障，建議記取	1.目前備援現況為兩條線路、兩張 100G 卡版，可在 BCP 演練中模擬事故發生情況。

	其經驗，避免爾後再發生同樣問題。	2.今年的 BCP 演練計畫中，已模擬區網 ASR 至 TANet 骨幹中斷之情況。
11	資安事件通報事件平均處理時間為 1.29 小時，通報率為 99.89%，建議改善之。	資安事件通報率已提升至 100%，平均處理時間小於 1 小時。
12	建議明年度協助完成連線學校之 IPv6 連線及 EDUROAM 之建置 。	1.協助樹人家商無線漫遊建置。 2.所有連線單位有配發 ipv6 之單位皆已完成 Peer IP 與路由設定。 3.明年度預計請尚未申請 IPv6 網段之單位儘速申請。
13	臺大網路技術能量高，能發現諸多區網運作之盲點，並提供相關建議改善之，針對此建議部分，建議能進一步將其規劃建置為區網中心之特色，諸如協助建立 TANet 黑名單、技服黑名單等，並協助成立資安健診輔導推動小組，來協助面對共同問題，共同防禦，共享資源等等。	因區網自身人力有限，擬規劃結合有意願之網管與有資安基礎之學生，共同組成網路與資安健診推動小組，可從校內各系所開始試行，進而推廣至連線單位及其他區網中心。

附表 1：區網網路架構圖

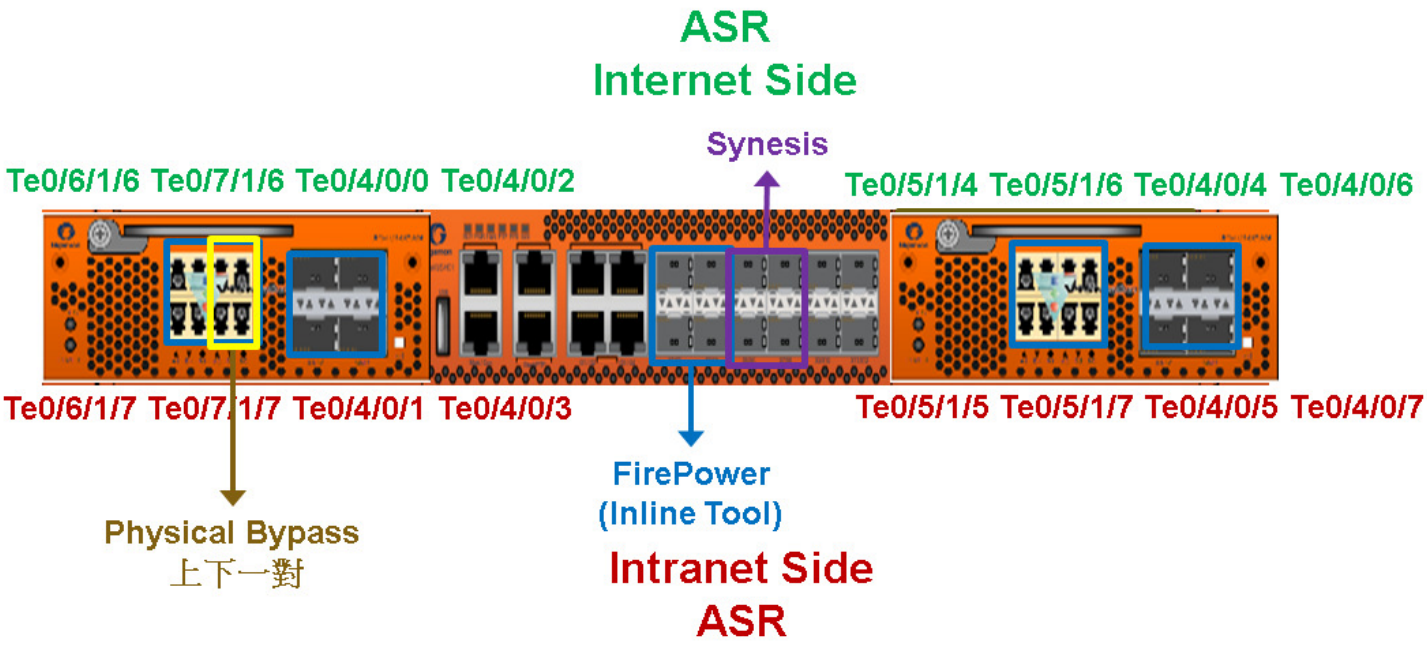
一、區網與連線單位(含縣(市)教育網路、連線學校、其他連線單位等)、TANet、Internet(Peering)的總體架構圖



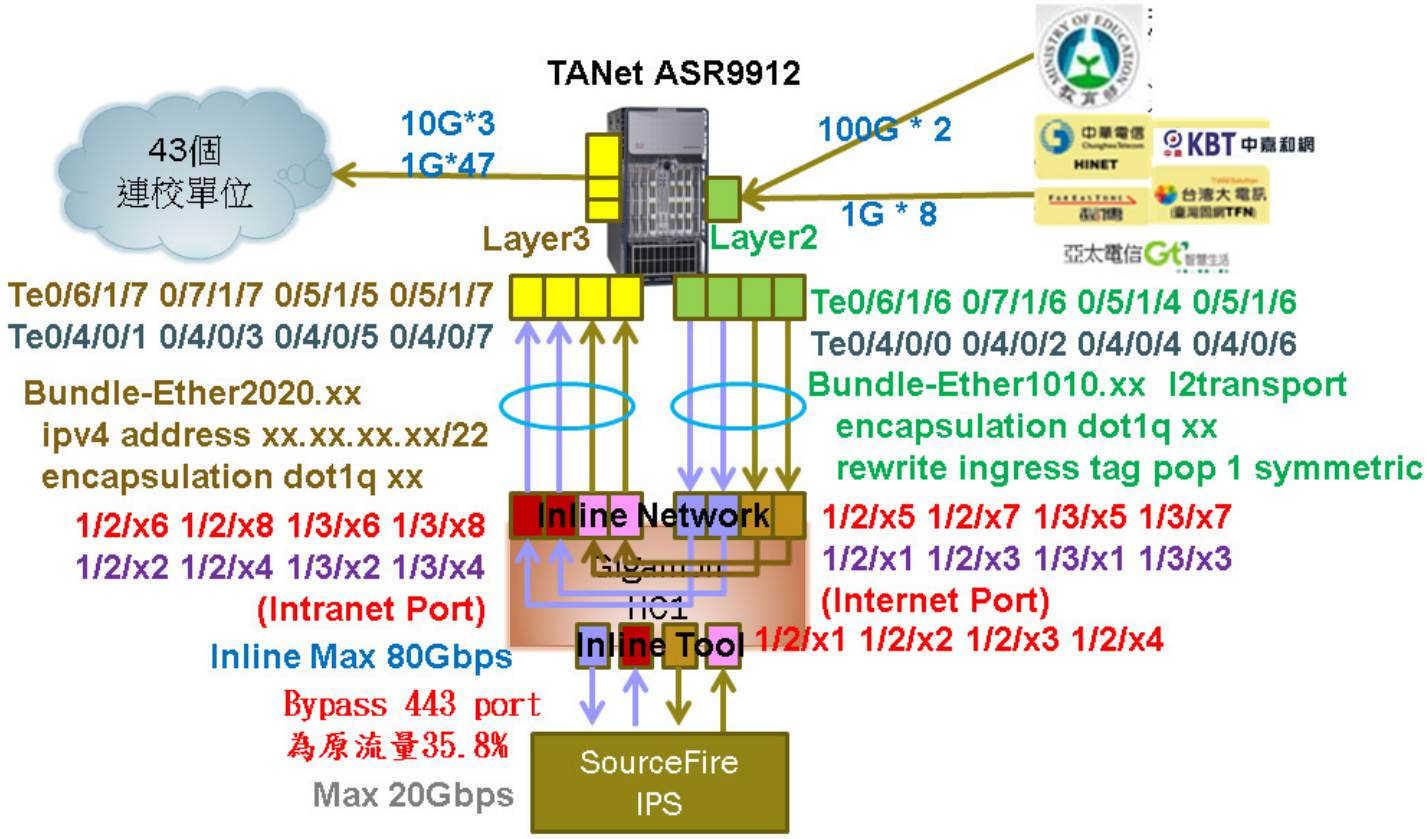
二、 網路配合各種應用架構(如連線分流、頻寬管理)或資安架構(防火牆、IDS/IPS/WAF)

的規劃或實際運作架構

三、 Gigamon 分流器接線架構圖



四、區網 ASR 與 Gigamon 分流器詳細接線架構圖



附表 2：連線資訊詳細表

1.請以**電路服務商**分列填寫，若單位/學校有多條連線但為同一供應商，請填寫一列合計頻寬，若有多供應商之連線，每一供應商填寫一列，寫多列個別填寫多列。

2.表格可自行調整。

		單位/學校名稱	電路頻寬(合計)	電路服務商	備註
縣(市)教育網中心	1.	臺北市	20G	亞太	
	2.	臺北市	20G	中華	
	3.				
	4.				
	5.				
	6.				
大專校院	1.	國防大學（復興崗校區）	1G	中華	
	2.	國防醫學院	1G	台灣固網	
	3.	國立臺灣大學	10G	Dark Fiber	
	4.	國立臺灣大學醫學院附設醫院	1G	中華	
	5.	國立臺灣師範大學(公館校區)	2G	中華	
	6.	國立空中大學	1G	中華	
	7.	國立臺北護理健康大學	1G	中華	
	8.	國立臺灣藝術大學	1G	亞太	
	9.	國立臺灣藝術大學	1G	中華	
	10.	國立臺北藝術大學	1G	中華	
	11.	國立臺北商業大學	1G	中華	
	12.	銘傳大學	1G	中華	
	13.	實踐大學	1G	中華	
	14.	臺北醫學大學	1G	台灣固網	
	15.	真理大學台北校區	1G	台灣固網	
	16.	大同大學	1G	遠傳電信	
	17.	龍華科技大學	1G	中華	
	18.	宏國德霖科技大學	1G	中華	
	19.	亞東技術學院	2G	遠傳電信	
	20.	致理科技大學	1G	中華	
	21.	黎明技術學院	1G	中華	
	22.	康寧大學	1G	中華	
	23.	華夏科技大學	1G	中華	
	24.	私立明志科技大學	1G	遠傳電信	
	25.	臺北海洋技術學院	2G	遠傳電信	

	26.	德明財經科技大學	1G	中華	
	27.	法鼓文理學院	1G	中華	
	28.	臺北市立大學	1G	臺灣智慧光網	
	29.	國防部軍事情報局軍事情報學校	1G	亞太	
	30.	臺北科技大學	10G	中華	
	31.	臺北基督學院	1G	台灣固網	
	32.	臺灣科技大學	10G	Dark Fiber	
高中職校	1.	國立臺灣師範大學附屬高級中學	1G	亞太	
	2.	臺北市私立育達高級商業家事職業學校	1G	中華	
	3.	臺北市私立協和祐德高中	1G	臺灣智慧光網	
	4.	臺北市私立復興實驗高級中學	1G	臺灣智慧光網	
	5.	臺北市私立開平餐飲職業學校	1G	中華	
	6.	桃園縣光啟高級中學	1G	中華	
	7.	新北市南山高級中學	1G	中華	
	8.	新北市私立徐匯高級中學	1G	中華	
	9.	新北市清傳高級商業職業學校	1G	中華	
	10.	新北市東海高級中學	1G	中華	
	11.	新北市私立樹人高級家事商業職業學校	1G	中華	
	12.	新北市能仁高級家事商業職業學校	1G	中華	
	13.	大同高中	1G	中華	
國中小學	1.	國立臺北教育大學附設實驗國民小學	1G	臺灣智慧光網	
	2.				
	3.				
	4.				
	5.				
	6.				
非學校之連線單位 (不含 ISP)	1.	新北市立圖書館	1G	中華	
	2.	中華民國高級中等學校體育總會	1G	中華	
	3.	財團法人大學入學考試中心	1G	Dark Fiber	
	4.	中華民國學生棒球運動聯盟	1G	台灣固網	

	5.	國家地震中心	1G	Dark Fiber	
	6.				
連接 TANet	1.	臺北主節點	100G		單 100G 介面
	2.	新竹主節點	100G		單 100G 介面
	3.				
	4.				
其他連線	1.				
	2.				
	3.				
	4.				
	5.				
	6.				