113 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）

113 年 11 月 6 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 1,802,000 元 2.教育部補助計畫金額：新臺幣 1,802,000 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 1,161,625 元，執行率 64%。
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： 0 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(110-112)經費使用達成率及本(113)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)。

1. 前 3 年度(110-112)經費使用達成率及本(113)年度預計達成率

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
110	1,792,000	1,788,692	0	99.82%	99.82%
111	1,792,000	1,240,866	529,918	69%	99%
112	1,792,000	1,131,871 (10月底)	49,307	95%	98% (預估)
113	1,802000	1,161625 (10月底)	67,143	95%	98% (預估)

2.檢討歷年度達成率。(如有經費繳回，請述明原因)。

110 年網路與資安助理皆是滿聘，達成率達 99.82%

111 年因資安助理 4/31 離職，112 年 1 月新任助理到職，達成率僅 69%。

112 年 2 月新任網管助理到職，需繳回一個月人事費，預估達成率約 95%

113 年因網管助理 3/31 離職，5 月新任助理到職，需繳回一個月人事費，預估達成率約 95%

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(110-112)及本(113)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)。

1.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。

2.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)資安事件調查與分析。

(3)DDoS 異常通報與回覆

(4)網路異常分析與監控。

3.檢討歷年度人事經費運作

110 年網路與資安助理皆是滿聘，達成率達 99.82%

111 年因資安助理 4/31 離職，112 年 1 月新任助理到職，達成率僅 69%。

112 年 2 月新任網管助理到職，需繳回一個月人事費，預估達成率約 95%

113 年因網管助理 3/31 離職，5 月新任助理到職，需繳回一個月人事費，預估達成率約 95%

四、114 年度經費與人力營運規劃(預估)。

1.114 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： 114 年 1 月 1 日至 114 年 12 月 31 日	
計畫經費總額：1,900,000 元，向本部申請補助金額：1,900,000 元，自籌款： 0 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)	41,156	13.5	555,606	1.薪資預算含年終獎金 1.5 個月。 2.第二年碩士薪資
	行政助理勞保費雇主(網管)	3,586	12	43,032	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。
	行政助理健保費雇主(網管)	2,045	12	24,540	
	行政助理勞退雇主(網管)	2,520	12	30,240	
	二代健保補充保費(網管)	1,303	1	1,303	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)	47,500	13.5	641,250	薪資預算含年終獎金 1.5 個月。
	行政助理勞保費雇主(資安)	3,914	12	46,968	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)	2,347	12	28,164	
	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)	1,503	1	1,503	年終獎金 2.11%之二代健保補充保費。二代健保補充保費為 47,500*1.5*2.11%=1,503。
			小計	**1,407,310**	
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	176	432	76,032	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
		120	500	60,000	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	1,000	12	12,000	區網中心相關主機等維護費，預計每月約 1000 元*12 個月，以 12,000 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	6,0000	1	6,0000	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	60,000	1	60,000	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	51,510	1	51,510	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	**462,690**	
三、設備及投資	電腦及周邊設備	30,000	1	30,000	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	**30,000**	
				1,900,000	

2. **人力規劃與工作執掌如下**:

(1) 計中主任：周承復 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：史詩妤

(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	33	13	1	6	連線單位總數： 54
	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		29	13	1	6	
		10G(含)以上	1	4				
	其他(如 ADSL 等)							
	連線電路小計		1	33	13	1	6	54
	連線頻寬合計		80G	69G	13G	1G	6G	連線頻寬總計：

	(電路實際租用頻寬加總)						169
	連線頻寬比率	47%	41%	8%	1%	3%	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	60G + 100G
			連線頻寬(中華)	ipv4 + ipv6:20G	
			連線頻寬(東豐)	ipv4 + ipv6:20G	
			連線頻寬(中研院 Dark Fiber)	ipv4 + ipv6:1000G	
	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.	台北市立圖書館	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.	中央氣象署	1G	
	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)	3	3Gbps	
	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：0.06小時。 (2)應變處理平均時數：0.23小時。 (3)事件處理平均時數：2.23小時。 (4)通報完成率：100%。 (5)事件完成率：100%。 3. 3、4級資安事件通報： (1)通報平均時數：0.1小時。 (2)應變處理平均時數：0小時。 (3)事件處理平均時數：0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：1.01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：100%。 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：98%。

(三)區域網路中心維運事項辦理情形及目標

項目	113辦理情形	114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) 。	6/28 第一次區網會議 出席率:94.5% (實體+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。	100% 骨幹線路與設備皆正常	目標: 99.9%
(3)連線學校之網路妥善率。	99 % 中華電信斷線持續四小時，影響 11 個連線單位。	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:17門 (實做課程 10門) 每堂課平均參與人數: 66人	暑期課程:10門 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: 97% 高中以下及其他單位: 90%	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。	2024/04: 遠傳 Peer 電	技術文件分享: 完成

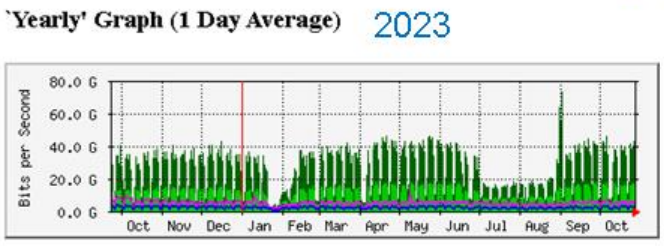
●建立區網路維運管理機制。 ●協助連線學校網路的維運或障礙排除(含諮詢) 。 ●建立資安防護或弱掃服務(含諮詢)。 ●建立連線學校相關人員聯繫管道及聯絡名冊。	路 2G 升速 3G 2024/05: 市網新增 100G Dark Fiber 2024/08: 新連線單位: 淡江大學 2024/10: 新連線單位: 臺北市圖書館	3 份以上網路資安文件撰寫 推廣網路品質監控系統: 建置於 3 個單位以上 使用區網連線學校基礎資料更新情況進行評核與審查: 每年完成 5 個單位
(7)服務滿意度。	整體服務滿意度: 85.4%	整體服務滿意度: 90%
(8)其他:		

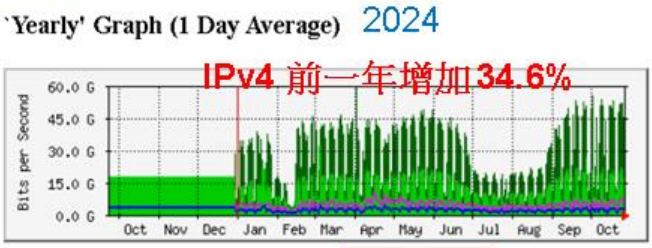
貳、請詳述貴區網中心之網路連線、網管策略及具體辦理事項(網路管理)

說明:1.113 年度網路管理維運具體辦理事項。
2.114 年度網路管理營運方針。

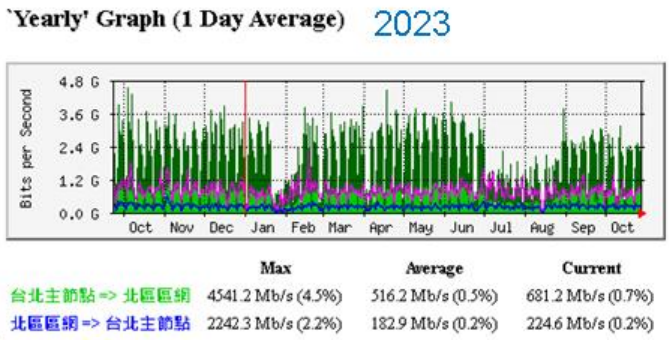
1.113 年網路流量使用狀況:

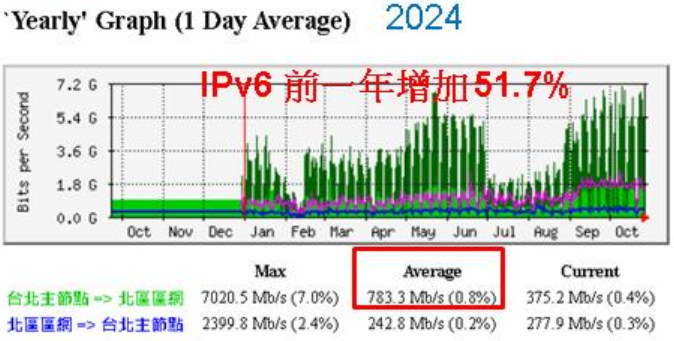
IPv4 流量





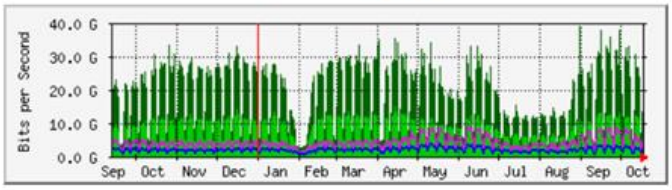
IPv6 流量





IPv4 流量

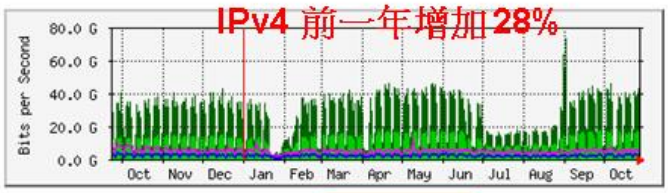
`Yearly' Graph (1 Day Average) 2022



	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%)

`Yearly' Graph (1 Day Average) 2023

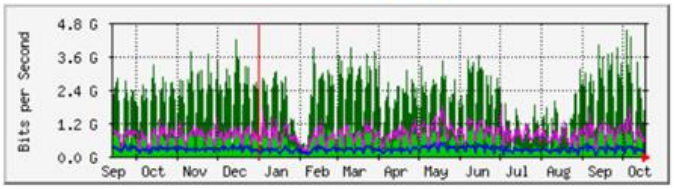
IPv4 前一年增加28%



	Max	Average	Current
InterNet => 北區區網	73.4 Gb/s (73.4%)	10.1 Gb/s (10.1%)	14.8 Gb/s (14.8%)
北區區網 => InterNet	13.1 Gb/s (13.1%)	1958.7 Mb/s (2.0%)	2298.1 Mb/s (2.3%)

IPv6 流量

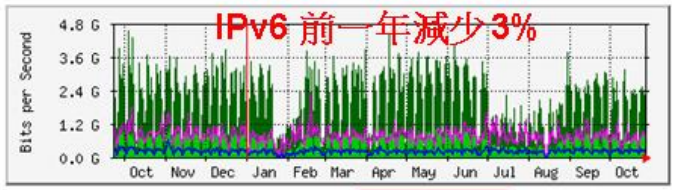
`Yearly' Graph (1 Day Average) 2022



	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%)

`Yearly' Graph (1 Day Average) 2023

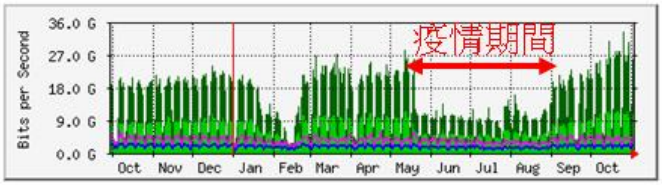
IPv6 前一年減少3%



	Max	Average	Current
台北主節點 => 北區區網	4541.2 Mb/s (4.5%)	516.2 Mb/s (0.5%)	681.2 Mb/s (0.7%)
北區區網 => 台北主節點	2242.3 Mb/s (2.2%)	182.9 Mb/s (0.2%)	224.6 Mb/s (0.2%)

IPv4 流量

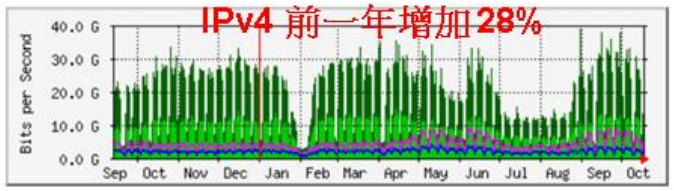
`Yearly' Graph (1 Day Average) 2021



	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%)

`Yearly' Graph (1 Day Average) 2022

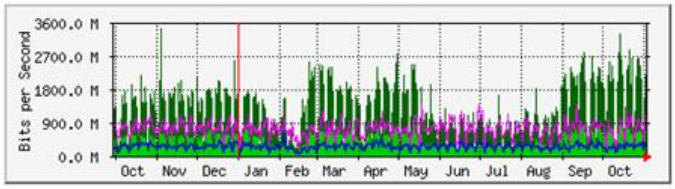
IPv4 前一年增加28%



	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

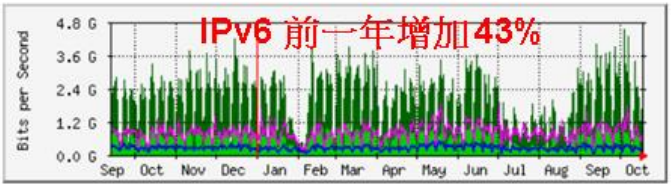
`Yearly' Graph (1 Day Average) 2021



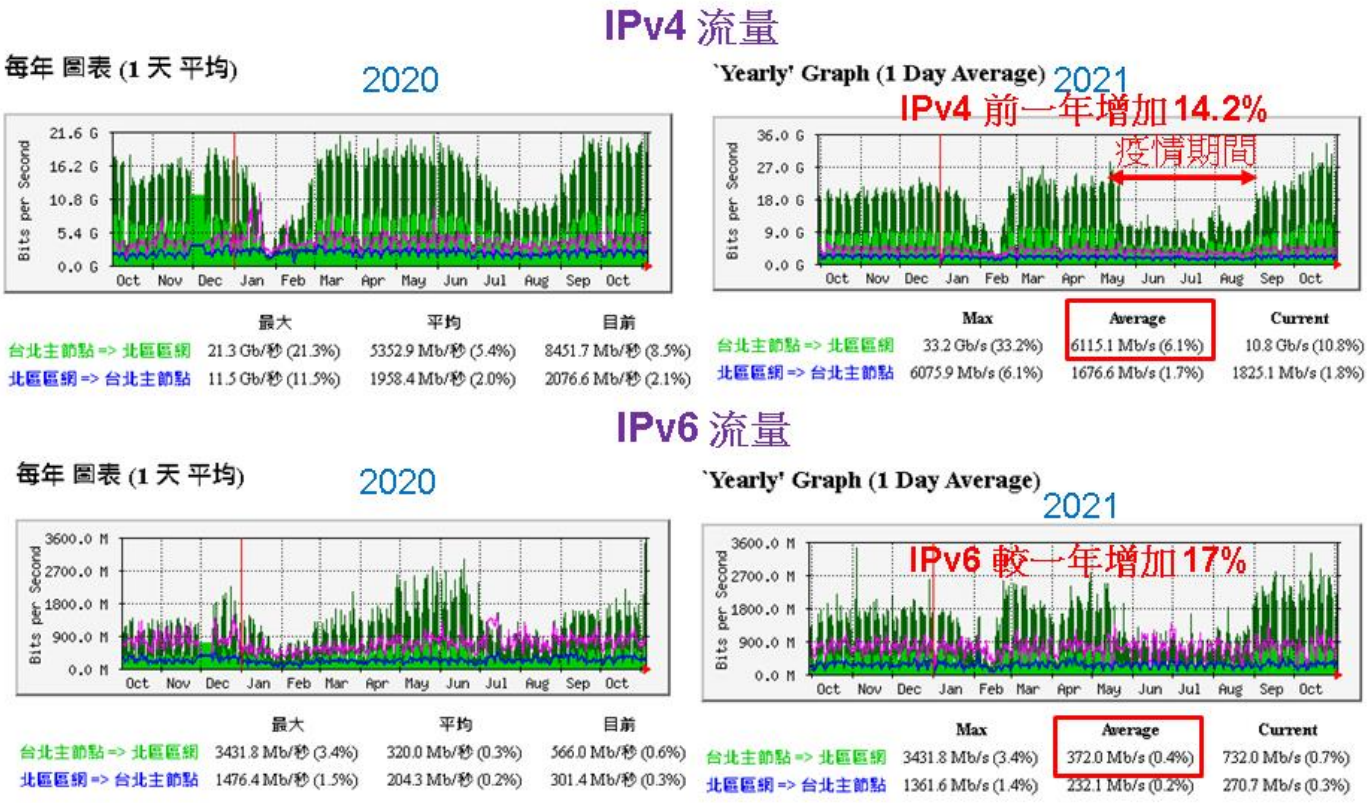
	Max	Average	Current
台北主節點 => 北區區網	3431.8 Mb/s (3.4%)	372.0 Mb/s (0.4%)	732.0 Mb/s (0.7%)
北區區網 => 台北主節點	1361.6 Mb/s (1.4%)	232.1 Mb/s (0.2%)	270.7 Mb/s (0.3%)

`Yearly' Graph (1 Day Average) 2022

IPv6 前一年增加43%



	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%)



2.113 年區網骨幹網路電路異動資訊:

2024/04: 遠傳 Peer 電路 2G 升速 3G

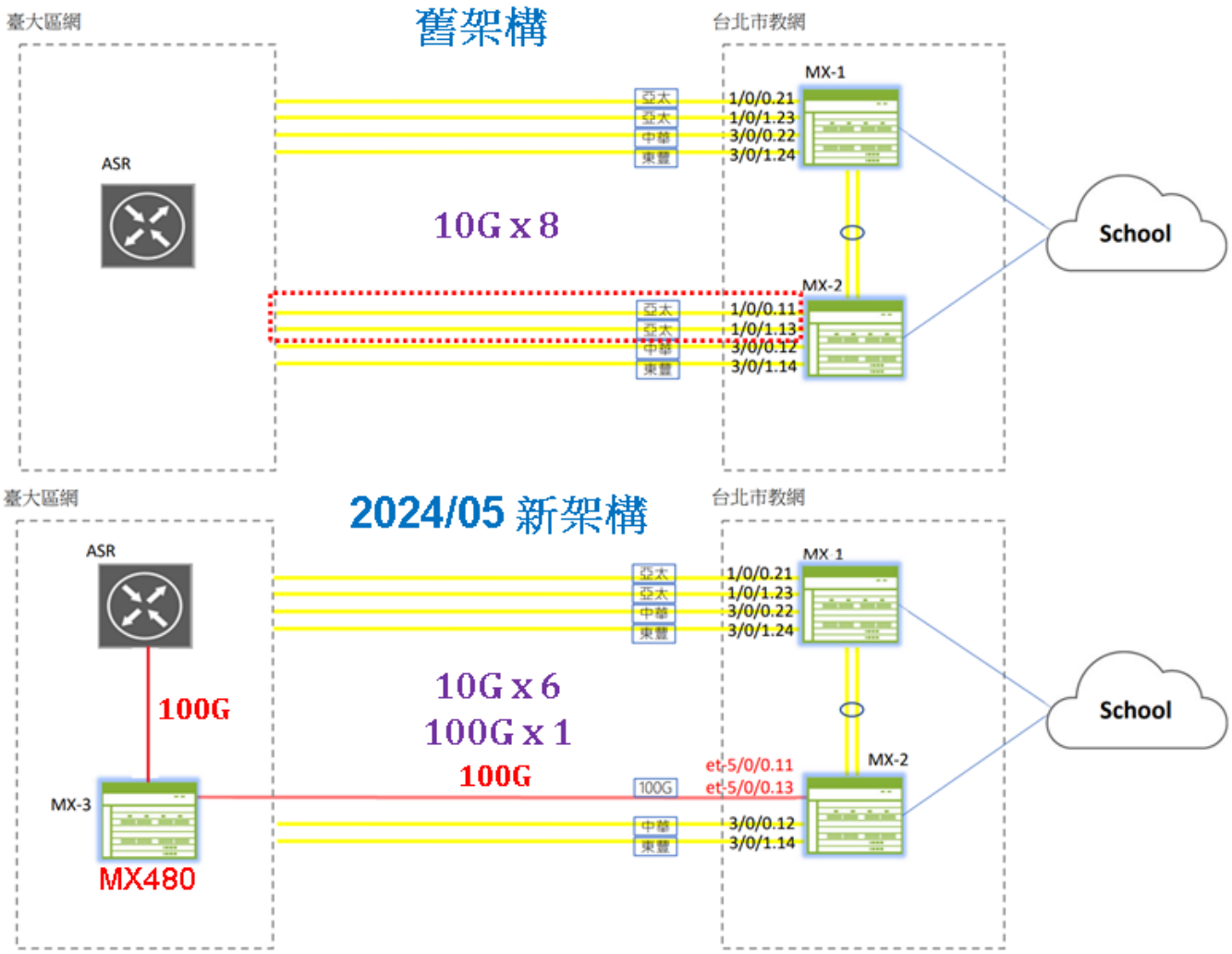
2024/05: 市網新增 100G Dark Fiber

2024/08: 新增連線單位: 淡江大學

2024/10: 新增連線單位: 臺北市圖書館

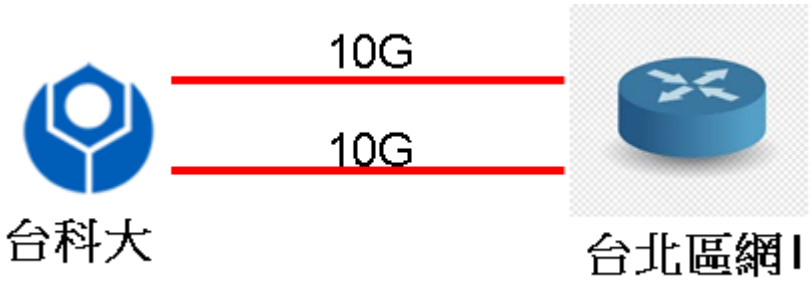
3. 市網新增 100G Dark Fiber

經教育部協調，借用中研院所屬市網至台大 Dark Fiber 兩蕊光纖，使用 100G 頻寬直連，為配合目前 10Gx8 之 Equal Cost Multi Path 架構，100G 線路切成兩個 Vlan 使用



4.連線學校: 臺科大使用 2 蕊暗光纖達成頻寬 10G x 2

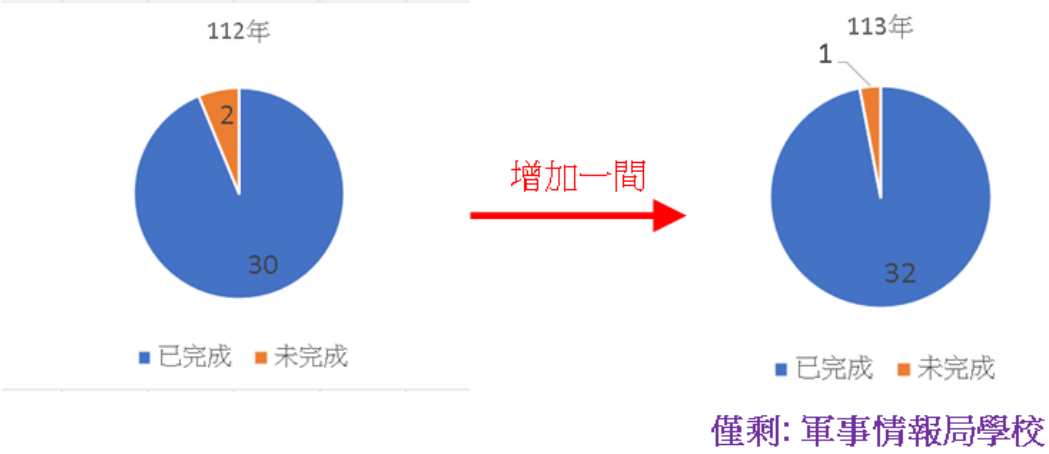
2 蕊光纖 Dark Fiber、每單蕊光纖 10Gbps



使用單蕊光纖 Transceiver、SFP 成套(一對)

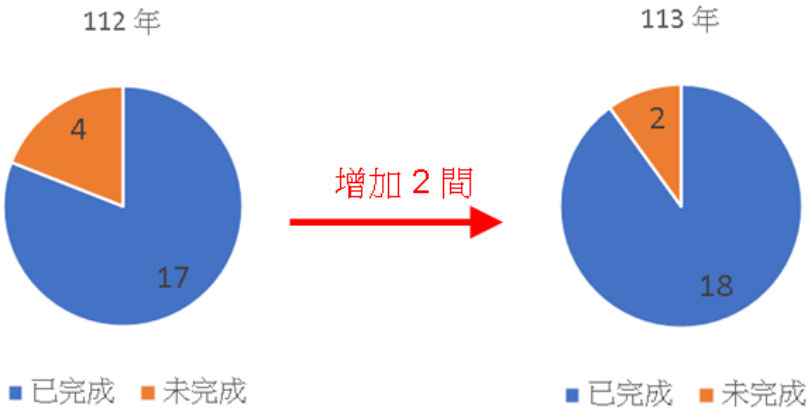
5. IPv6 連線單位完成率統計

(1) 大專院校: 33 間



僅剩: 軍事情報局學校

(2) 高國中小及其他單位: 20 個



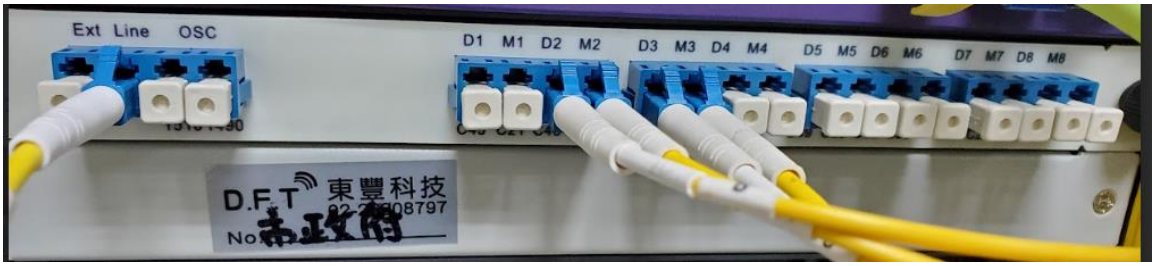
僅剩: 中華民國學生棒球運動聯盟、國家地震中心

6. DWDM Passive 使用單蕊暗光纖可達成 10G x 8

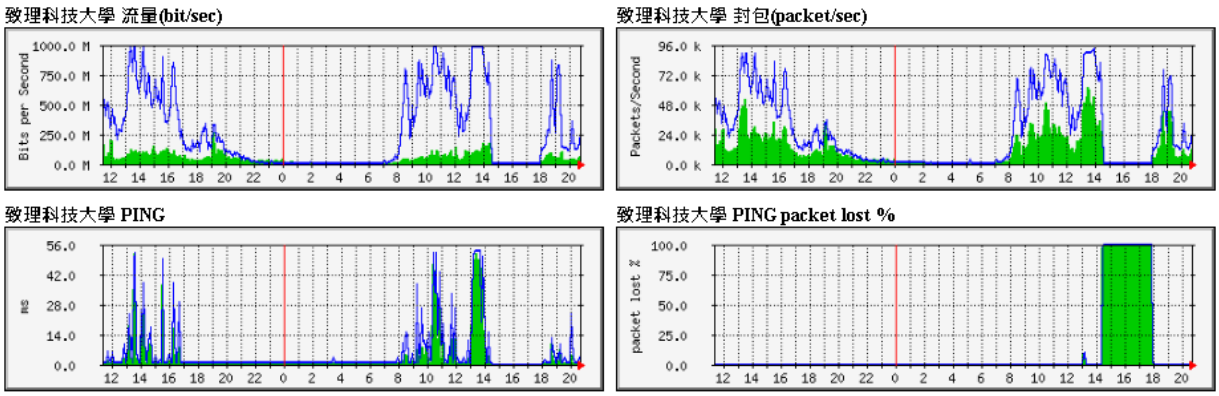
台北市網電路供應商東豐科技使用 DWDM Single Dark Fiber

8 Channels: Use 16 Waves

頻寬可達 10G x 8



7. 2024/09/24 中華電信斷線持續四小時以上



共有 11 間學校受到影響:

致理科技大學、龍華科技大學、台北護理健康大學

臺灣藝術大學、德明財經科技大學、國立空中大學

國防大學管理學院、東吳大學(城中校區)

宏國德霖科技大學、康寧大學-台北校區、臺灣大學醫學院校區

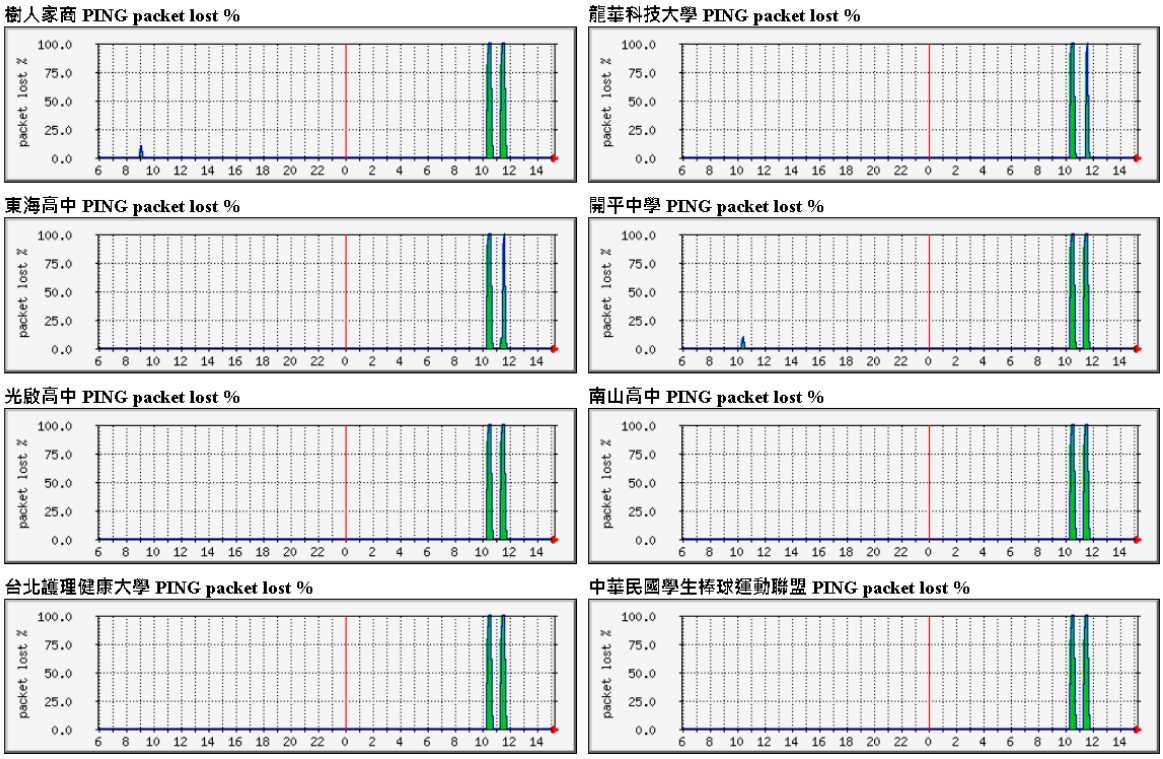
中華電信檢討報告回覆，因設備設定異常造成

8. 2024/02/18 ASR9K 韌體升級斷線過程

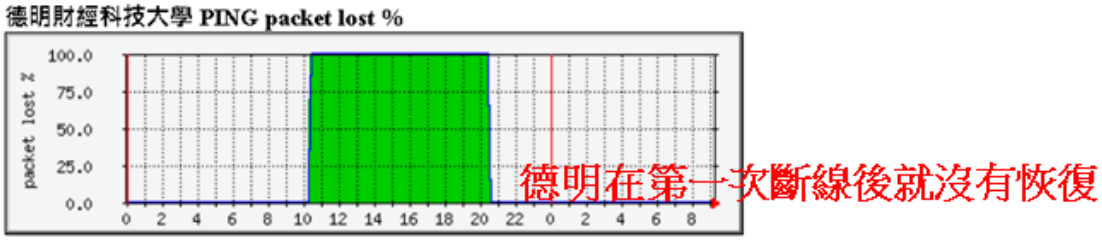
●正常斷線時間共兩次

10:26 ~ 10:37 (11 分鐘)

11:27 ~ 11:39 (12 分鐘)

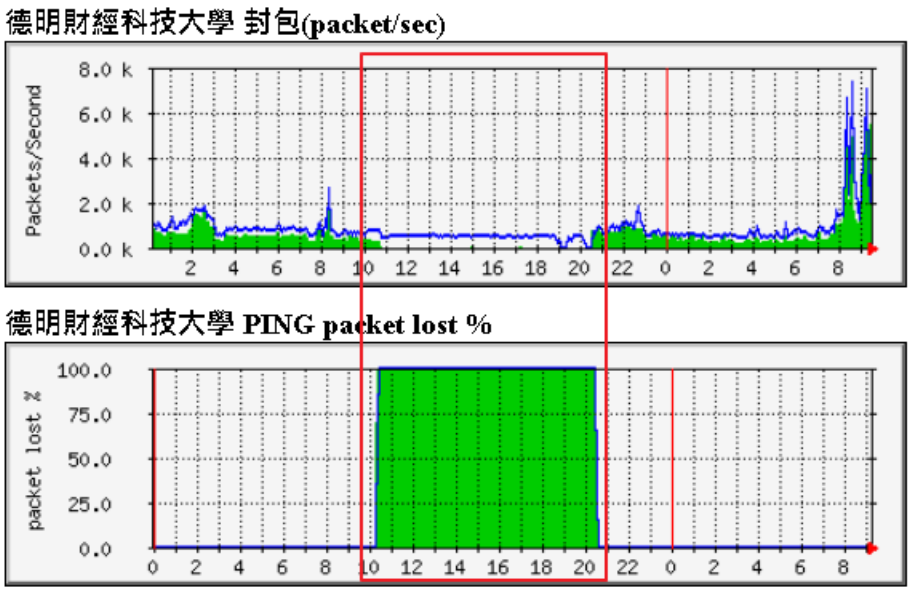


●德明科大



斷線期間，台大路由器仍持續有 Out 封包流量?

原因: 因為持續有收到 Peer IP 192.192.7.57 之 ARP 封包，因此路由持續往德明科大介面傳送



●德明科大介面封包側錄 @區網端

確認: 無 Vlan Tag -> 電路設定正常

持續有收到德明科大 Fortinet 之 ARP 封包　德明 to 台大 電路正常

	Vlan	Source	Destination	Protocol	Length	Info
181		Fortinet_09:00:11	Broadcast	ARP	60	Who has 192.192.7.57? Tell 192.192.7.58
182		Cisco_55:63:22	Fortinet_09:00:11	ARP	60	192.192.7.57 is at 04:6c:9d:55:63:22
665		Fortinet_09:00:11	Broadcast	ARP	60	Who has 192.192.7.57? Tell 192.192.7.58
666		Cisco_55:63:22	Fortinet_09:00:11	ARP	60	192.192.7.57 is at 04:6c:9d:55:63:22
1111		Fortinet_09:00:11	Broadcast	ARP	60	Who has 192.192.7.57? Tell 192.192.7.58
1113		Cisco_55:63:22	Fortinet_09:00:11	ARP	60	192.192.7.57 is at 04:6c:9d:55:63:22
1543		Fortinet_09:00:11	Broadcast	ARP	60	Who has 192.192.7.57? Tell 192.192.7.58
1544		Cisco_55:63:22	Fortinet_09:00:11	ARP	60	192.192.7.57 is at 04:6c:9d:55:63:22
1944		Fortinet_09:00:11	Broadcast	ARP	60	Who has 192.192.7.57? Tell 192.192.7.58
1945		Cisco_55:63:22	Fortinet_09:00:11	ARP	60	192.192.7.57 is at 04:6c:9d:55:63:22
2403		Fortinet_09:00:11	Broadcast	ARP	60	Who has 192.192.7.57? Tell 192.192.7.58
2404		Cisco_55:63:22	Fortinet_09:00:11	ARP	60	192.192.7.57 is at 04:6c:9d:55:63:22
2881		Fortinet_09:00:11	Broadcast	ARP	60	Who has 192.192.7.57? Tell 192.192.7.58
2882		Cisco_55:63:22	Fortinet_09:00:11	ARP	60	192.192.7.57 is at 04:6c:9d:55:63:22
3335		Fortinet_09:00:11	Broadcast	ARP	60	Who has 192.192.7.57? Tell 192.192.7.58
3336		Cisco_55:63:22	Fortinet_09:00:11	ARP	60	192.192.7.57 is at 04:6c:9d:55:63:22

●測試小結:

區網端: 路由器、SFP 介面、路由設定皆正常

德明端: 路由器、IP 設定皆正常

電路商: 中華電信:

德明 to 台大 電路正常

台大 to 德明 電路 ？ 待釐清

●最終結果

台大電信機房中華電信設備 Zyxel 機器斷電重開後恢復正常

該設備不明原因，ASR 韌體升級第一次斷線後，僅有單向流量(德明 to 台大)正常，台大 to 德明 封包無法正常傳送

To Do: 要求中華電信更換或調整 Zyxel 設備避免再次發生

9.113 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)區網網路與資安課程: 10 場以上

(6)區網課程 Lab 實做課程: 佔 50%以上

(7)技術文件分享: 完成 3 份以上網路資安文件

(8)使用區網連線學校基礎資料更新情況進行評核與審查: 每年完成 3 個單位

10. 區網服務 VM 主機群 (網頁主機、WAF 防護、MRTG、Cacti)由 Vmware ESXi 移轉至 Proxmox Virtual Environment(PVE)

- 先聊聊 Vmware ESXi 之壞話

1.嚴格的硬體支援清單且淘汰快速

■RAID

僅支援硬體 RAID 卡 (不支援主機板/軟體式)

硬體 RAID 卡 Server 最低價 Dell R750 $157,614 (政府採購網)

■網卡

Realtek 網卡從未被正式支援

V6.x

100Mbps 皆不支援、僅支援 1G 以上網卡

僅支援至 6.x

Broadcom BCM5751、BCM5721

Intel E1G42ET Dual Port (82576)

僅支援至 7.x

Intel Ethernet Server Adapter X520-DA2

■CPU

IBM Server x3650 無法升級 v6.7

ASUS BP1AF 無法升級 v7

Dell Precision Tower 5810、OptiPlex 990 無法升級 v8

2.VMware 之近況

■2022 博通 Broadcom 宣佈以 610 億美元(溢價 50%）併購 Vmware (Broadcom

市值 2200 億)

博通已分別收購軟體公司 CA Technologies，賽門鐵克企業端安全業務

■2023/11　收購完成後一周裁減 VMware 人力，據稱超過 2,000 人。未經證實的消息指出博通以不續工作簽證為手段，迫使外籍工程師主動離職。

https://www.reddit.com/r/vmware/comments/1b1sah4/broadcom_silent_layoffs_email_to_vmware_about_40/?rdt=61195

■2023/12 取消現有合作夥伴關係，只接受下單量大的經銷商作為新的合作夥伴

https://www.ithome.com.tw/news/160549

峰儀業務 Cors 最近提到 Vmware 已經不提供教育版 License

■2024/01 終結 56 項 VMware 產品，包括 vSphere Hypervisor，以簡化產品、減少研發成本

https://www.thestack.technology/vmware-is-killing-off-56-products-including-vsphere-hypervisor-and-nsx/

■2024/01 VMware 宣布不再單獨銷售永久授權，未來改採用訂閱制

https://blogs.vmware.com/cloud-foundation/2024/01/22/vmware-end-of-availability-of-perpetual-licensing-and-saas-services/

■2024/02 End Of General Availability of the Free vSphere Hypervisor (ESXi 7.x and 8.x)

https://kb.vmware.com/s/article/2107518?lang=en_US

■2024/03 以 38 億美元將 VMware 遠端存取技術用戶端運算部門（End-User Computing，EUC）出售給私募基金 KKR，包含企業平臺 Workspace ONE 整合終端管理（Unified Endpoint Management，UEM）、旗艦桌機及應用程式虛擬化平臺 Horizon

https://www.ithome.com.tw/news/161589

● 功能強大、友善硬體支援 Proxmox Virtual Environment(PVE)

■ Open Source Solution
Linux Debian + QEMU/KVM + LXC(Linux Container)

■ 硬體相容性佳

相容於 Linux Debian Kernel

支援 Realtek 網卡

支援 100Mbps 網卡

支援舊型 PCI 介面網卡 (主流: PCI-E/PCI Express)

PCI Passthrough 限制少

支援 USB Mouse/Keyboad

支援 USB Audio/Video (USB Camera)

● Vmware vCenter 能做到的 Proxmox VE 都支援

■ VM Clone
■ Full Clone
■ VM Template:
Link Clone

■ Cluster 中控台

不需安裝額外軟體 (vCenter Appliance)

節省後續維運升級之困擾

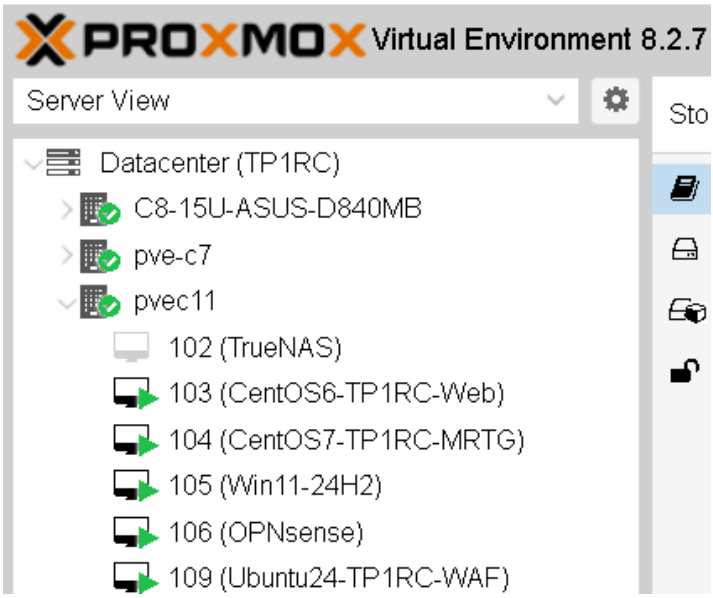
每台 Node 皆可當成中控台

避免 vCenter 當機或所在 Host 當機

■ VM Migrate: (VMware vMotion)

Node 主機搬移

Storage 搬移



■HA 高可用性

■不需額外付費，內建即支援

Proxmox Backup Server

增量備份、資料壓縮、重複資料刪除

備份 VM Disk 內容檢視，不需還原即可取出檔案

內建 Email Notification

11. 區網網管會議

●113 年第一次網管會議出席率: 94.5%

●實體與線上會議同步進行

●安排連線單位輪流技術交流分享

臺北醫學大學 --北醫大雙校區機房整建與資安健檢經驗分享

台大醫院 -- 從 syslog 到網路聯防機制

大考中心 -- 教育部資通安全稽核技術與經驗分享

台師大 -- 大考中心 - 教育部資通安全稽核技術與經驗分享

臺北海洋科技大學 – 校園網路骨幹建置與宿舍網路建議經驗分享

12. “高中體育總會”離開 TANet 事件過程與檢討

●因高中體育總會多次未參區網會議，去電要求出席會議，並回覆連線單位相關表單。

●112 年 12/08 高中體育總會發文申請退回 TANet 網段(退出 TANet)

中華民國高級中等學校體育總會 函

地址：臺北市中山區朱崙街20號13樓

受文者：國立臺灣大學

發文日期：中華民國112年12月8日
發文字號：112高體（六）字第1120203440號
速別：普通件
密等及解密條件或保密期限：
附件：

主旨：有關鈞部配給本會「臺灣學術網路」，擬申請繳還案，請鑒核。

說明：

一、經查，旨揭IP發放係由2010年1月1日鈞部代理發放予本會，委由國立臺灣大學（臺大區網中心）管理。

二、本會用戶網段為140.131.203.0/24，現因本會長年不再使用，擬提出申請繳還。

●TANet 之優勢

Pubic IP 很多

提供許多資安防護方案:

IPS 防護偵測

DDoS 防護與清洗

不當資訊防護

網頁與系統弱掃服務

●TANet 之限制與缺點

需遵循教育部及連線單位使用規範，遵循資安法及資安稽核

電路費較租用 ISP 服務貴上 10 倍

Peer 電路 300M: 每月一萬

光世代 300M: 每月 $999

網路服務品質相較 ISP 無明顯優勢:

國際頻寬壅塞: 2023/09 ~ 2024/04

GCP(Google Cloud Platform)@新加坡: 部分單位無法連線 2023 /03 ~ 2024/07

LOL 英雄聯盟遊戲延遲 (RTT 過高) : 2024/10 發生，尚未解決

■實際現況

許多連線學校早已租用 ISP 服務當成 TANet 備援線路

●補充資訊

■GCP(Google Cloud Platform) 無法連線

測試網址與 IP:

網址	IP	是否可正常連線
https://www.ici.nccu.edu.tw/	43.254.18.15	OK
https://affair2.tksh.ntpc.edu.tw/wp/president/	35.213.190.90	
https://www.su101.net/	35.213.134.67	
http://learningcollaboration.org/	35.213.173.85	
http://www.shoulder-elbow.org.tw/	35.213.154.88	
https://mindsetsonline.co.uk/	35.214.18.63	
https://icis2023.aisconferences.org/	34.174.71.254	OK
https://amcis2023.aisconferences.org/	34.174.71.254	OK
https://pacis2023.aisconferences.org/	34.174.71.254	OK
https://wuzhoucollege.nqu.edu.tw/	85.187.128.49	OK
https://www.palaugov.pw/	35.213.182.202	
https://data.aseanstats.org/	35.213.140.188	
https://tjcit.org/	35.213.140.188	
https://globalinnovationchallenge.org/	35.210.206.35	
https://jasp-stats.org/	35.214.239.75	
https://suricata.io/	35.212.0.44	
https://kamatiam.org/	35.215.102.40	

無法連線網段: GCP @新加坡: 35.208.0.0 255.240.0.0

■TANet Telstra 電路國際頻寬壅塞過程

2023/10 ~ Telstra 開始壅塞

2023/11 教育部期末會議報告提出

2024/04/19 Telstra 50G 擴充至 70G

2024/04/23 Cogent, Telstra Load Balance

2024/05/06 取消 Load Balance

2024/06 教育部期中會議回覆: 已經有進行路由調整,僅對 Cogent 發送 TANet 特定網段， Telstra 僅有一路在特定時間才有壅塞情形

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

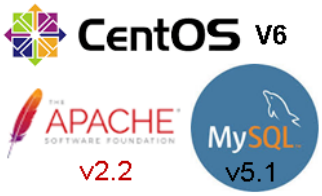
甲、110~113 年度資安事件統計

	110	111	112	113
1、2級資安事件處理				
通報平均時數	0.05 小時	0.001 小時	0.07 小時	0.06 小時
應變處理平均時數	0.86 小時	0.086 小時	0.25 小時	0.23 小時
事件處理平均時數	1.42 小時	0.087 小時	2.88 小時	2.23 小時
通報完成率	99.89 %	100 %	100 %	100 %
事件完成率	100%	94.48%	100%	100%
3、4級資安事件通報				
通報平均時數	無	無	無	0.1
應變處理平均時數	無	無	無	0
事件處理平均時數	無	無	無	0
通報完成率	無	無	無	100%
事件完成率	無	無	無	100%
資安事件通報審核平均時數	0.55小時	0.003小時	0.83小時	1.01小時
資料更新完整校數	100%	56.52%	100%	98%

乙、區網網頁新架構

(1)網站安全 Web Site Security

* 2021/09 教育部公文要求網頁**全面導入HTTPS**
* 2022/08 美國國會議員裴洛西訪台，遭受對岸網軍進行**網頁置換攻擊**
* 2023/12 國立大專院校**資安攻防演練計畫(網頁滲透測試)**
* 台北區網I網頁現況



* 網站潛在風險
  * CentOS v6 + PHP v2 + MySQL v5 → 過於老舊、存在漏洞
  * Let's Encrypt免費憑證 Certbot 程式 → 不支援 CentOS v6
  * 支援動態程式網頁:網頁後台管理系統、首頁公佈欄、連線單位資訊更新 → 維護人員更迭、程式未妥善更新

(2)可能解決方法

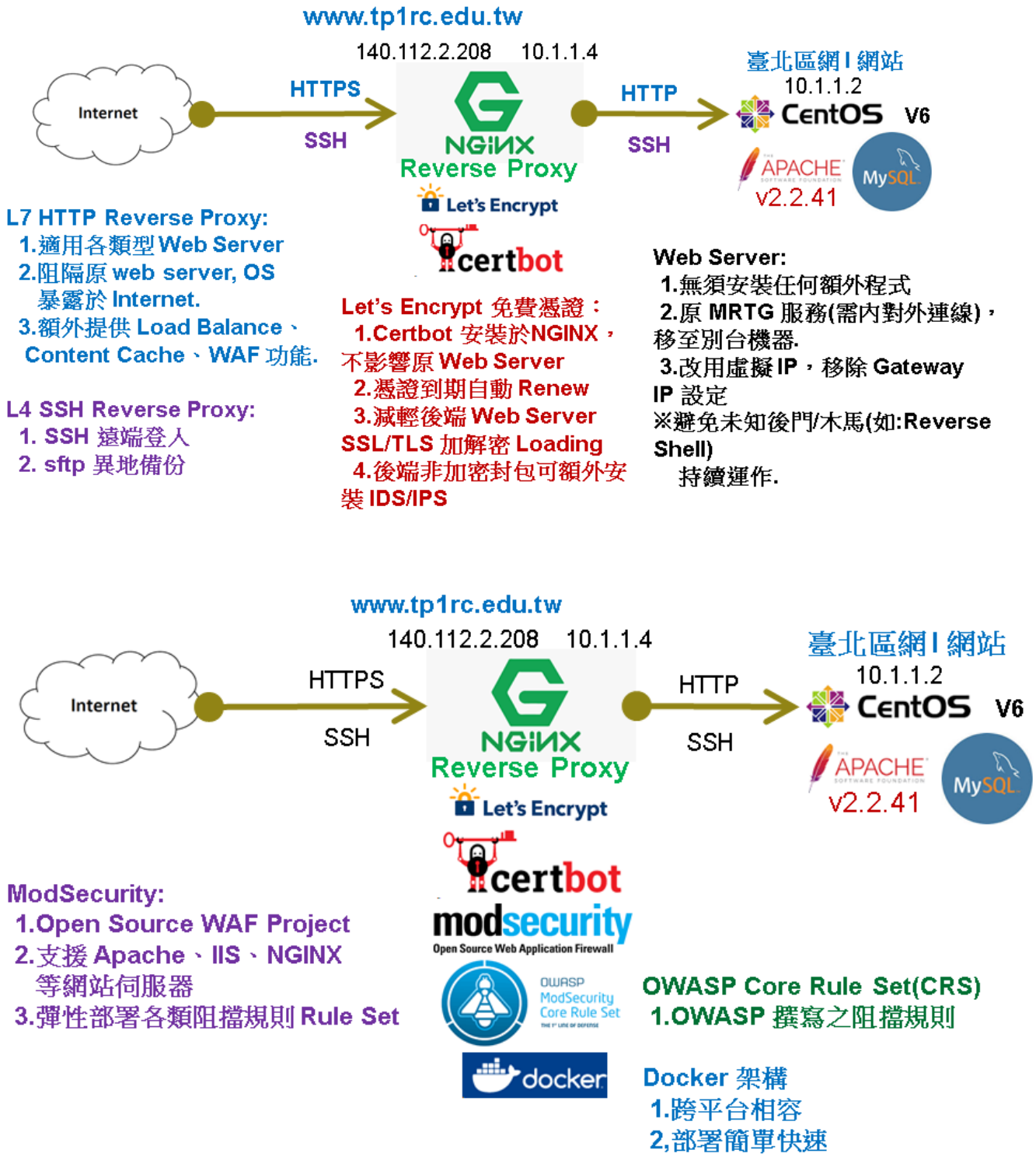
因 PHP v2 部分程式語法與新版 v8 不同，所有程式需重新改寫: 人力不足

改為純靜態網頁: 無後台管理功能、無動態程式功能: 網頁功能受限

改用公版網頁範本: 網頁功能受限、範本風格雷同

導入 WAF 網頁防火牆: 經費有限

(3)區網網頁新架構:



(4)L7 HTTP Reverse Proxy 阻隔原網站 Web Server, OS 暴露於 Internet

原始網站

L7 Reverse Proxy

(5)區網弱掃報告

原始網站

Alerts distribution

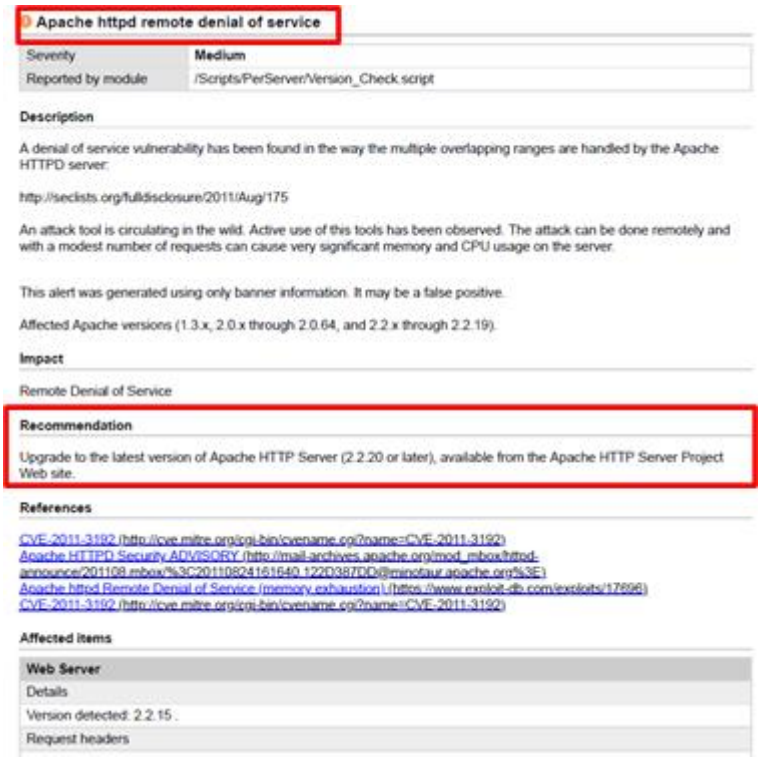
Total alerts found	15
High	0
Medium	3
Low	7
Informational	5

L7 Reverse Proxy

Alerts distribution

Total alerts found	13
High	0
Medium	2
Low	7
Informational	4

共減少 2 個弱點



Apache httpd remote denial of service

Severity	Medium
Reported by module	/Scripts/PerServer/Version_Check.script

Description

A denial of service vulnerability has been found in the way the multiple overlapping ranges are handled by the Apache HTTPD server.

http://seclists.org/fulldisclosure/2011/Aug/175

An attack tool is circulating in the wild. Active use of this tools has been observed. The attack can be done remotely and with a modest number of requests can cause very significant memory and CPU usage on the server.

This alert was generated using only banner information. It may be a false positive.

Affected Apache versions (1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19).

Impact

Remote Denial of Service

Recommendation

Upgrade to the latest version of Apache HTTP Server (2.2.20 or later), available from the Apache HTTP Server Project Web site.

References

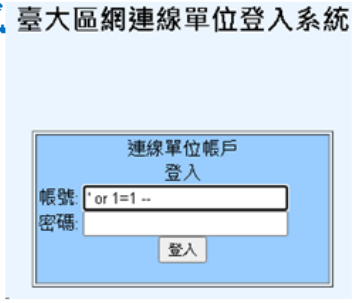
CVE-2011-3192 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192)
Apache HTTPD Security ADVISORY (http://mail-archives.apache.org/mod_mbox/httpd-announce/201108.mbox/%3C20110824161640.122D387DD@minotaur.apache.org%3E)
Apache httpd Remote Denial of Service (memory exhaustion) (https://www.exploit-db.com/exploits/17696)
CVE-2011-3192 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192)

Affected items

Web Server
Details
Version detected: 2.2.15 .
Request headers

(6)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

(7)網頁弱掃軟體測試

台北區網 I 網站	Acunetix (成大弱掃平台)	IBM AppScan	Burp Suit Web Vulnerability Scanner
高風險	0	1	0
中風險	2	12	3
優點	清楚的修正建議	1.掃到最多問題 2.清楚的修正建議	
缺點	掃到問題不多，且部分有誤判情況	部分問題等級也許是低	1.掃到問題不多 2.修正建議不是很清楚

丙、輔導系所網站快速導入 WAF 防護機制

■ 系所網站面臨問題

網站 OS、Web Server、動態程式，版本老舊無法升級，需重新安裝、程式重新改寫

原網站開發人員離職、無維護廠商

經費不足

■ 快速導入 WAF 防護機制

◆ 維持原網頁主機實體環境與 IP 網路架構

阻擋校外直接連線網頁主機(IPS 封鎖)，僅限校內存取

不需將網頁主機搬移至計中 VM 租賃區

計中 VM 租賃區規定: 主機弱掃、網站弱掃、原碼掃描、EDR(CrowdStrike)

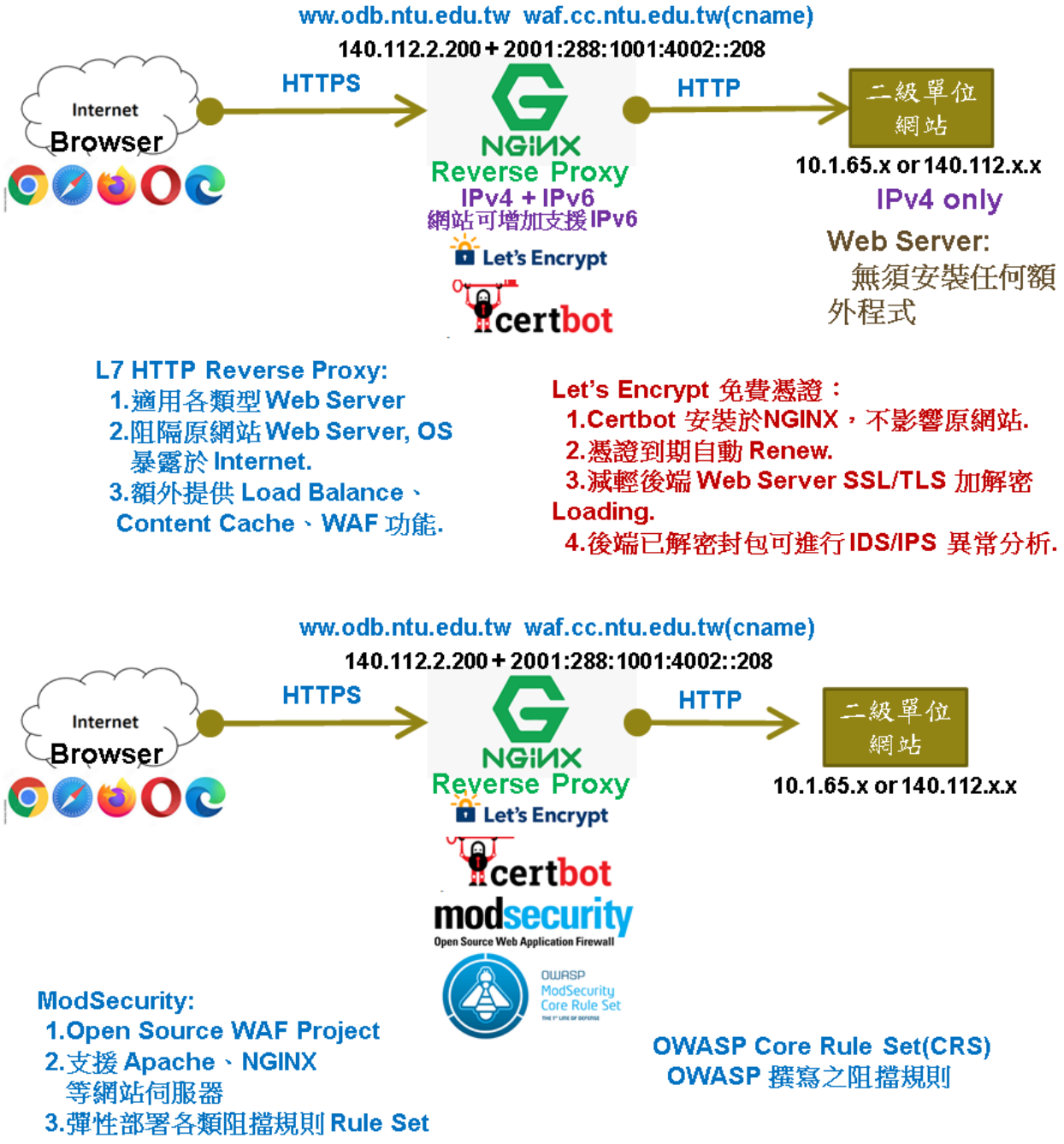
◆ 在校內可直接連線網頁後台、SSH、RDP

網頁管理後台不需通過 WAF 檢測，減少 WAF 規則誤擋

減輕 WAF 規則設定

不需在 WAF 設定 Port Forward for SSH, RDP

■ Open Source WAF 網頁防護架構



■ DNS 設定方法

原網站使用 DNS Alias Name 指向 waf.cc.ntu.edu.tw

www.odb.ntu.edu.tw IN CNAME waf.cc.ntu.edu.tw

設定 waf.cc.ntu.edu.tw 之 A Record 記錄

waf.cc.ntu.edu.tw IN A 140.112.2.x

原網站 IP

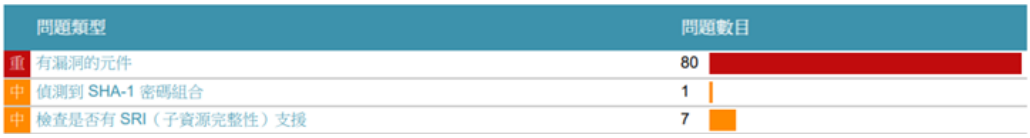
維持 140.112.x.x (IPS 封鎖，僅限校內存取)

改成 10.1.x.x

■ AppScan 掃描結果比較

* 原網站

* 導入 WAF 後



■ WordPress xmlrpc 程式 POST listMethod (成功阻擋)

Request

Pretty Raw Hex

```
1 POST /xmlrpc.php HTTP/1.1
2 Host: pc4.buda.idv.tw
3 Sec-Ch-Ua: "Chromium";v="123", "Not:A-Brand";v="8"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "Windows"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122
  Safari/537.36
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
  e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7
15 Priority: u=0, i
16 Connection: close
17 Content-Length: 95
18
19 <methodCall>
20   <methodName>
       system.listMethods
     </methodName>
21   <params>
22   </params>
23 </methodCall>
24
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 403 Forbidden
2 Server: nginx/1.24.0 (Ubuntu)
3 Date: Tue, 11 Jun 2024 09:14:24 GMT
4 Content-Type: text/html
5 Connection: close
6 Content-Length: 564
7
8 <html>
9   <head>
      <title>
        403 Forbidden
      </title>
    </head>
10  <body>
11    <center>
        <h1>
          403 Forbidden
        </h1>
      </center>
12    <hr>
      <center>
        nginx/1.24.0 (Ubuntu)
      </center>
13  </body>
14 </html>
15 <!-- a padding to disable MSIE and Chrome friendly error page -->
16 <!-- a padding to disable MSIE and Chrome friendly error page -->
17 <!-- a padding to disable MSIE and Chrome friendly error page -->
18 <!-- a padding to disable MSIE and Chrome friendly error page -->
19 <!-- a padding to disable MSIE and Chrome friendly error page -->
20 <!-- a padding to disable MSIE and Chrome friendly error page -->
21
```

■ Outbound Rules Test Directory Transversal

* https://ghp.ntu.edu.tw/icons/small/

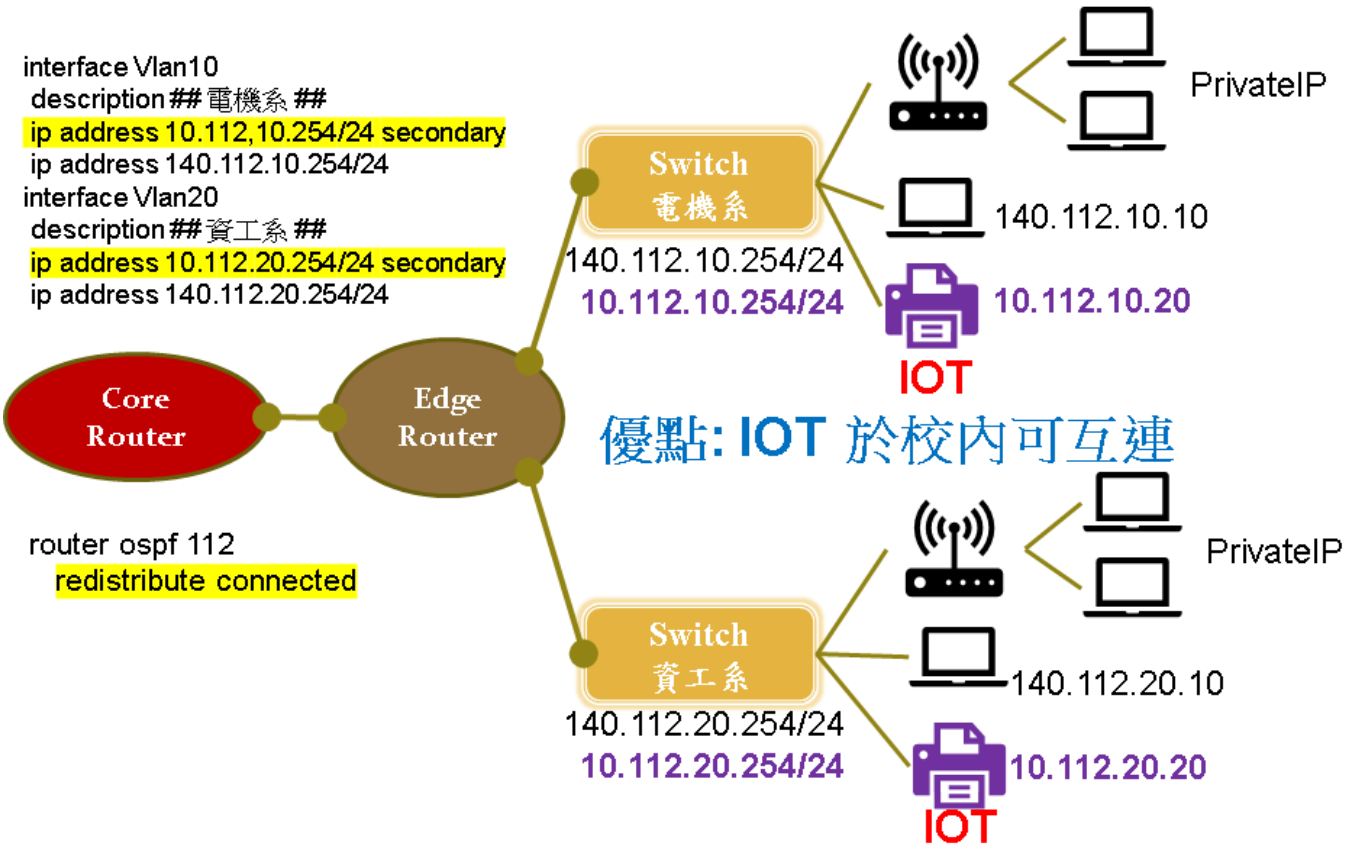
Index of /icons/small

Name	Last modified	Size	Description
Parent Directory		-	
back.gif	2004-11-21 04:16	129	
back.png	2007-08-28 18:53	181	
binary.gif	2004-11-21 04:16	134	
binary.png	2007-08-28 18:53	172	

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、113 年度區網課程(17 門)

分類	講題	講者	出席
資安	駭客攻擊手法深入探討	中華資安 林峰正	91
雲端	檔案不再雜亂無章:使用 Google Workspace 打造作流 (線上實做)	CloudMile 陳宏傑	80
系統	Proxmox VE 入門實作課程 (LAB 實做)	節省工具箱公司 技術總霖	37
雲端	Google Classroom 實際應用場景 (線上實做)	CloudMile 陳宏傑	48
雲端	解鎖工作效率新境界：Gemini for GWS 實戰應用做)	CloudMile 鄭浔元	77
法規	AI 著作權議題	胡中瑋律師	48
雲端	透過 AppScript Generative AI (Gemini API) 整理信件內容 (線上實做)	CloudMile 張家瑋	75
大數據	Elasticsearch 上 AI 與 ML 的說明與運用	集先鋒 Anthony 陳俊佑	77
資安	深入探討特權帳號管理系統整合運用	鉉迪資訊 資深技術顧問	80
雲端	無痛連結 Google Workspace, REST APIs（初階）	CloudMile 陳智聰	71
雲端	無痛連結 Google Workspace, REST APIs（進階）	CloudMile 陳智聰	55
系統	以 Pure Storage 平台來加速擁抱 AI 的驅動力	Pure Storage 蔣燚峰	53
資安	網站常見弱點檢測與修補(LAB 實做)	高于凱	46
網路	網管工程師必修課程 -- 網路設備常見規格、常用原理介紹	游子興、史詩妤	95
資安	常見的網站漏洞利用以及防禦介紹 (LAB 實做)	中華資安 蕭子修	68

資安	滲透測試 LAB 實作練習 (LAB 實做)	中華資安 蔡侑達	35
資安	常見網站弱點與修補方法 -- 以 WordPress 為例	陳思蘊、游子興	88

己、113 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。

庚、114 年度資安服務目標(實施措施)

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

肆、特色服務

一、請說明貴區網中心服務推動特色、辦理成效。

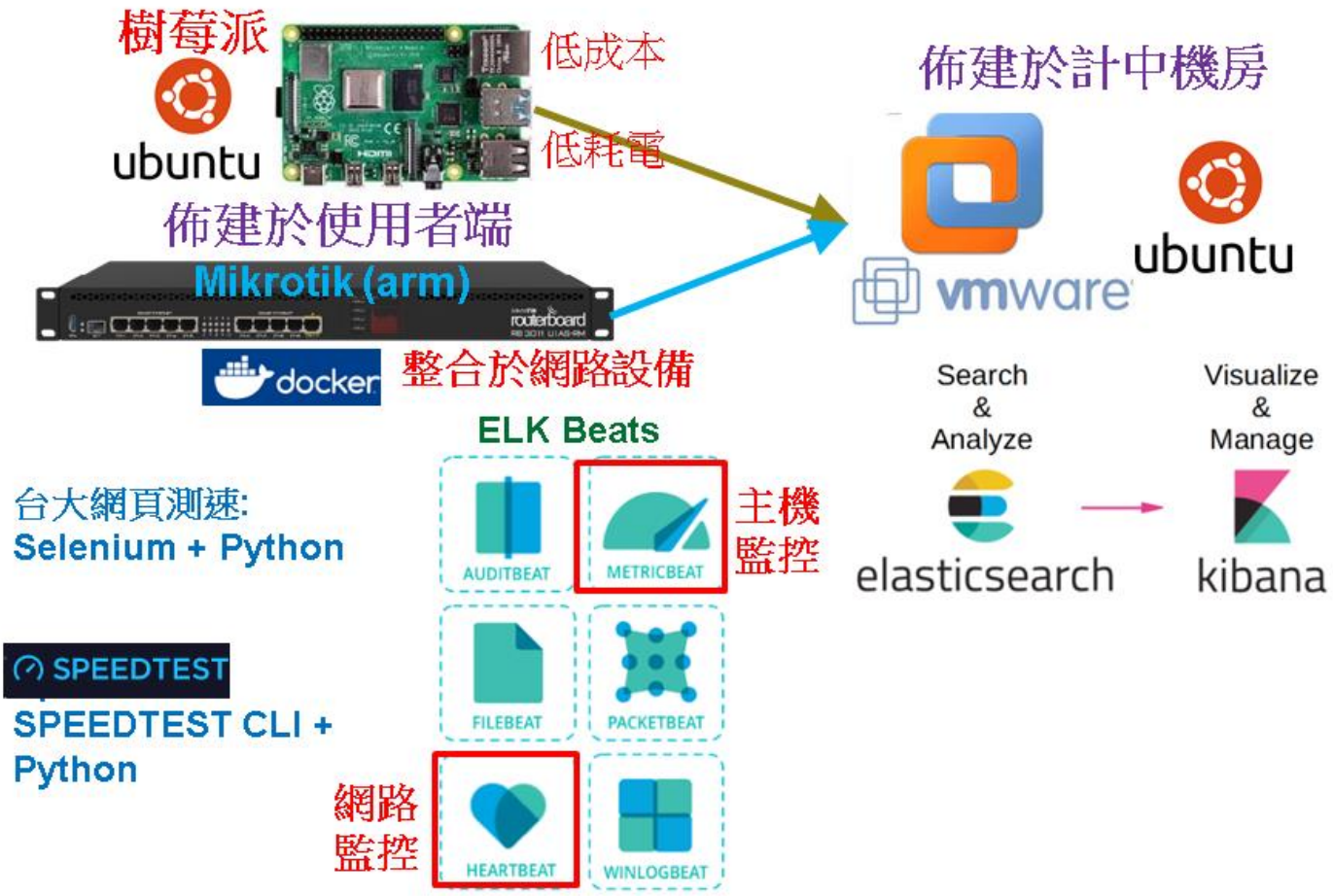
說明:1.113 年度服務特色辦理成效。

2.114 年未來創新服務目標與營運計畫。

3.創新特色議題 (對 TANet 網路或資安管理有助益之特色服務) 。

4.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



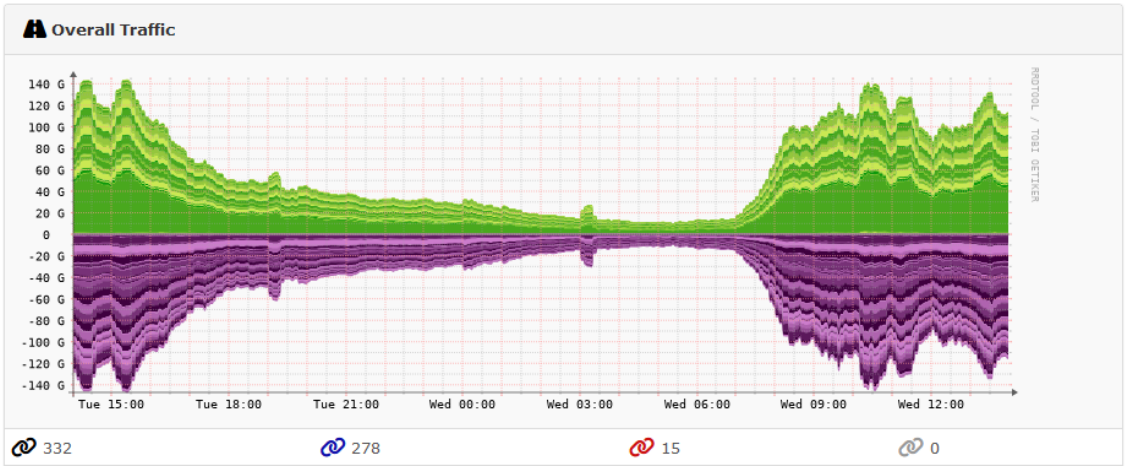
乙、架設 LibreNMS 提供區網連線單位網路品質監控

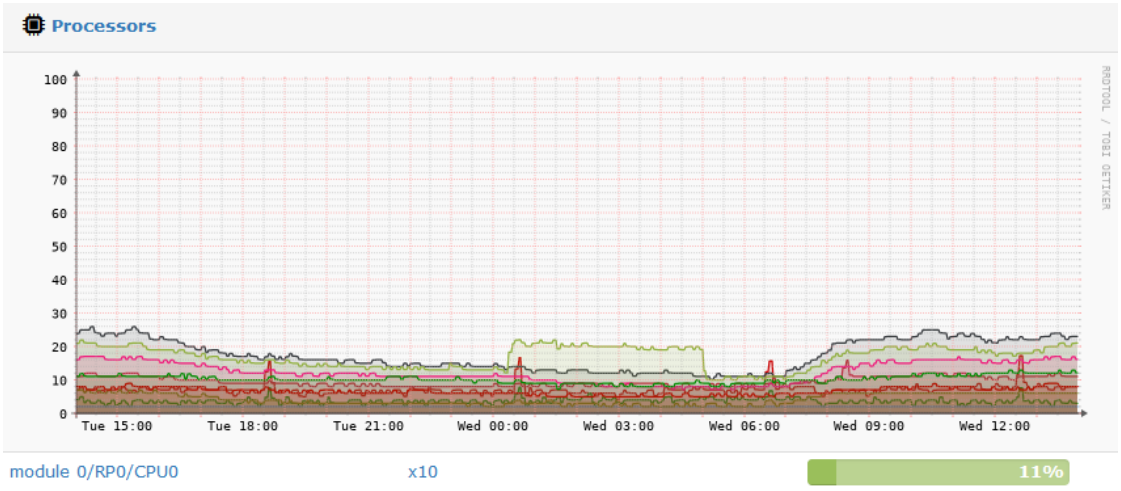
LibreNMS 透過 SNMP 蒐集區網 ASR 相關資訊

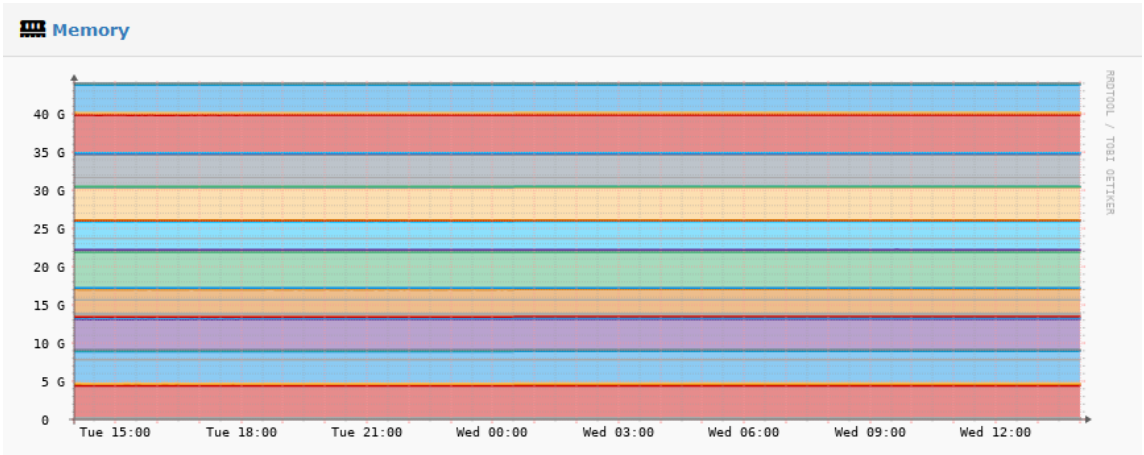
架設告警系統以即時偵測設備狀況與流量

建立即時流量圖表

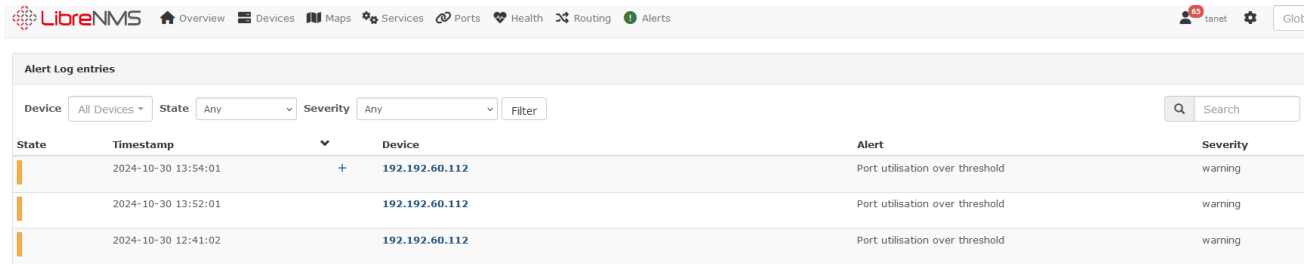
SNMP 蒐集區網 Router 資訊，以即時監測設備狀態與告警



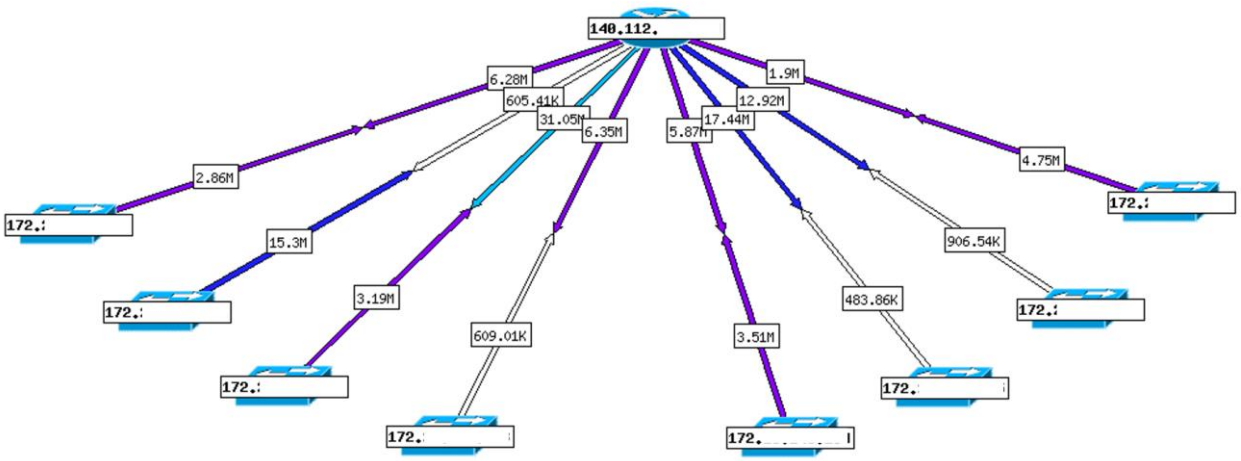




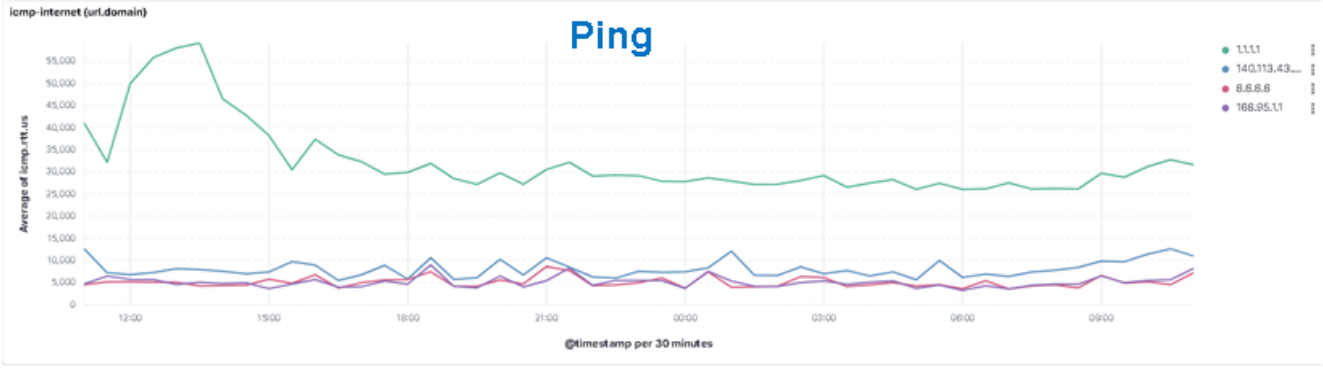
LibreNMS 自動告警機制，建立斷線、流量異常等信件、Line 告警

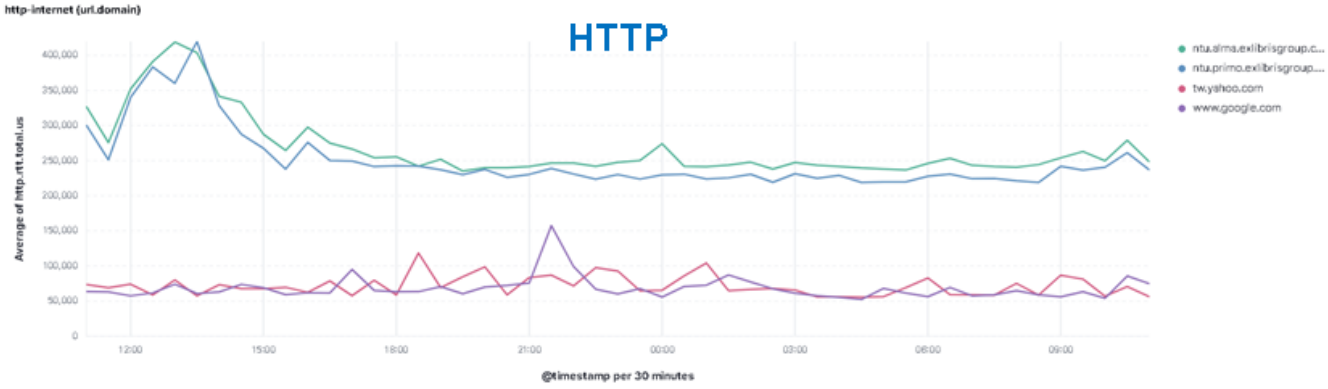


LibreNMS 可透過 WeatherMap 建立連線即時流量圖。預計後續架起該功能，以供查看。

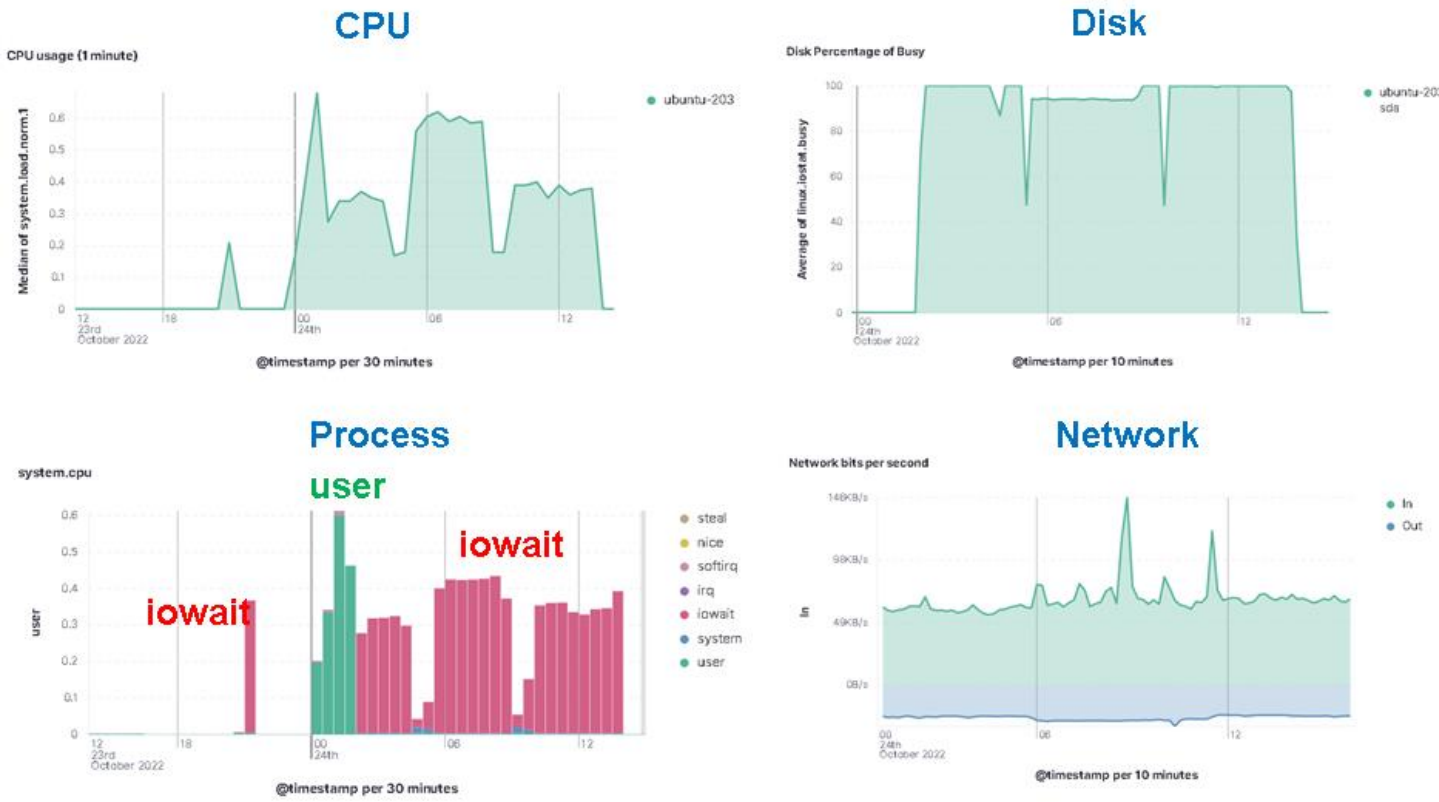


丙、ELK Heartbeat 網路監控





丁、ELK Metricbeat 主機監控



二、未來創新服務目標與營運計畫。

說明:1.114 年度創新服務目標與構想。

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

● 113 營運目標 達成報告

1.網路妥適率: 99.99%以上

達成，骨幹線路與設備皆正常 100%

2.區網網管會議出席率: 90%以上

達成，出席率 94.5%

3.大專院校 ipv6 使用率: 100%

未達成，僅剩一間學校(軍事情報局)

4.高國中小 ipv6 使用率: 80%以上

達成，使用率 90%

5.區網網路與資安課程: 10 場以上

達成， 共開設 17 門課程

6.區網課程上機實做課程: 佔 50%以上

達成， 線上與現場上機共開設 10 門課程

7.技術文件分享: 完成 3 份以上網路資安文件

達成， 區網會議、暑期課程共完成六份不同主題之技術文件。

8.推廣網路品質監控系統: 建置於 3 個單位以上

達成，目前建置在校內單位，但尚未推廣至連線單位。

因使用者端網路品質監控系統，需要布建實體設備至使用者端，目前的確僅在校內單位進行。但因為布建設備成本低廉，(Raspberry Pi 或 MikroTik hEX 約台幣 3 千元左右)，成果與效益非常不錯，因此於網管會議上分享此案例，連線單位可視需求自行建置。

9.使用區網連線學校基礎資料更新情況: 進行評核與審查

部分達成，目前由連線單位自行填報，尚未進行評核與審查，預計明年會特跌加強宣導。

●112 年評審委員建議與回覆

No	委員建議	回覆
1	2023/04/29 13:30 : 區網與臺北主節點不明原因中斷連線，2023/05/01 11:41 : 區網與臺北主節點不明原因中斷連	建議的改善方法如下: 1.100G 骨幹重要設備應有維護合約 2.100G 電路應有 SLA 合約與斷線罰款機制

	線，暫時開啟新竹主節點 100G 卡版，但此卡版原先異常狀況並未排除，導致線路斷斷續續故 障，建議未來故障原因查找應更有效能，縮短區網服務中斷時間，避免 影響使用者網路使用。	3.TANet 骨幹應有 24Hr 維運工程師，必要時候可進行異常通報與聯繫 4.區網路由器有單點失效風險，建議應建立 HA 機制
2	為避免網路節點發生單點故障，雖已自動連結其他主節點，建議可定期辦理 BCP 演練並確實執行演練檢討、分析及規劃未來精進方式。	因台大計算機中心已納入 ISO27001 驗證範圍，高風險業務每年會要求進行 BCP 演練。 本年度 BCP 演練主題，特別模擬台大區網骨幹路由器 ASR 9912 與 台北主節點實體光纖線路中斷，BGP 路由自動切換至新竹主節點，藉此演練路由備援機制是否正常運作。
3	建議針對防入侵設備檢視說明是否執行有 log 收集、分析及建立警告機 制，同時對零時差攻擊建議可收集相關資訊並隨時視狀況更新。	臺北區網 I 目前之資安防護，依照規劃屬於北區 ASOC 團隊之防護範圍，北區 ASOC 團隊使用 Cisco FirePower IPS 進行入侵偵測與攻擊防禦，設備皆有拋出 Log 給大數據分析系統進行收集、分析及自動告警機 制，大數據系統目前使用 ArcSight 與 ELK Stack 兩套系統同步進行分析。
4	針對 Reverse Proxy 程式碼是否檢視有無安全問題?來源為何?Patch 如何 及時更新?建議可審慎規劃及確實執行資安檢核。	Reverse Proxy 使用 NGINX(WebServer)、ModSecurity(NGINX Connectot)、OWASP CRS(Rule Sets) 三項套件組成。 NGINX 目前是市佔率第一名之 WebServer，並提供 Source Code 可供檢視，OWASP 是權威網站資安組織，定時公布知名之 OWASP Web Top 10 網頁弱點供大家參考，因此應無安全疑慮。 即時更新目前使用 Ubuntu 自動更新機制，使用 apt update + apt dist-upgrade 可即時更新有漏洞之套件。
1	已於 7 月辦理第一次區管會，預計在 12 月份召開第二次會議，兩次會議皆集中在下半年辦理；因此會議為與連線單位溝通協調之橋梁，建議爾後還 是以上下半年各召開一次為原則處理。	已進行改善，今年上半年的區網會議於 6/26 上半年舉行，連線單位出席率達 94.5%， 下半年之區網會議預計於 12 月舉行。
2	針對今年 DDOS 攻擊，建議未來可構思如何透過有效 SOP 以協助轄管連線單位更迅速解決問題。	臺北區網 I 目前之 DDoS 防護，依照規劃屬於北區 ASOC 團隊之防護範圍，北區 ASOC 團隊使用 Genie 威睿科技 及 Radware DefensePro 進行 DDoS 偵測與防禦。

		目前規劃之 SOP 如下: 1.Genie 使用 netflow 偵測 DDoS 之發生，自動發告警信件給區網網管人員。 2.區網收到告警通知後，通知被攻擊之連線單位，並同步使用大數據分析系統 ELK Stack 進行攻擊來源與目的封包分析。 3.依據分析結果與連線單位確認是否要自動進行清洗或直接於 區網路由器使用 ACL 進行阻擋。 4.依據討論決議進行自動進行清洗或 ACL 阻擋。
1	對整體區網與各連線學校的網路服務架構圖（含相關資安防護、CDN、分流…等各節點設備），能有完整的呈現，以利後續若有維運工作的檢視或研議網路運作效能評估時有詳實的參考文件。	已完成。 最新版網路架構圖已經加上網路分 流器、資安防護設備、TANet CDN 設備、不當資訊設備等，並更新線路頻寬等資訊，請參考文件第六頁。
2	對所提資安人員的工作任務有資安鑑識，是否為區網服務連線學校之工作，亦或僅限部分範圍，請再確認。	謝謝委員建議，目前區網資安人員在能力與時間上的確還無法做到資安鑑識與調查，目前主要是針對近期著名的資安事件進行事件分析與調查，因此工作項目已經更改成”資安事件分析與調查”。
3	對區網召開區管理會議時，其與連線學校或單位有何具體達成維運管理之 目的?	區網管理會議的目的有兩個: 1.連線單位相互認識與意見交流: 連線單位每學期藉由區網召開之管理會議，可相互認識、交換意見，瞭解各單位網管之工作與經驗分享。 2.技術精進與經驗交流: 去年開始，每次區網會議皆有安排一個連線單位，分享單位內網路管理政策與使用之網路設備，分享實用之網路技術與管理經驗
4	對有提供使用者端網路品質監控系統，其是否具推廣至各連線應用的能力，或僅為校內服務事項，請再確認。	使用者端網路品質監控系統，需要布建實體設備至使用者端，目前的確僅在校內單位進行。但因為布建設備成本低廉，(Raspberry Pi 或 MikroTik hEX 約台幣 3 千元左右)，成果與效益非常不錯，因此於網管會議上分享此案例，連線單位可視需求自行建置。
5	對所提測速有使用自行開發及中華電信 speed test 工具其間有差異，可否	網路連線速度測試目前的確有許多方法可供測試，https://www.speedtest.net/、台大測速

	評估何者較接近連線學校網路使用者實務連網的網速。	http://speed5.ntu.edu.tw/speed5/，TANet 今年也有開放測速程式 https://sp.tanet.edu.tw/。 以理論上而言，使用之測速程式伺服器越接近連線單位，才能測試出實際之連網速度，因此建議使用者多方測試後，再依照測試結果來判斷。
6	對教育部資安弱掃團隊所建構的工具可移至區網提供服務，建議評估導入為區網對連線學校的服務項目之一。	謝謝委員建議，此部分最近有與成大弱掃團隊確認，目前系統弱掃因版本授權因素，並未開放布建至區網端提供服務。 因此需要由連線單位提出申請後，直接由成本團隊遠端提供弱掃服務，區網端預計在年底之會議中也會加強宣導弱掃的申請方式與服務介紹。
7	對本年度區網維運相關工作任務的成果或執行過程，建議能有此範圍的檢討與建議，以為下年度精進作為	已完成，謝謝委員建議。 詳見 “6.基礎維運” 其中” 113 營運目標 達成報告” 章節。

●未來營運目標

1.網路妥適率: 99.99%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.區網網路與資安課程: 10 場以上

6.區網課程 Lab 實做課程: 佔 50%以上

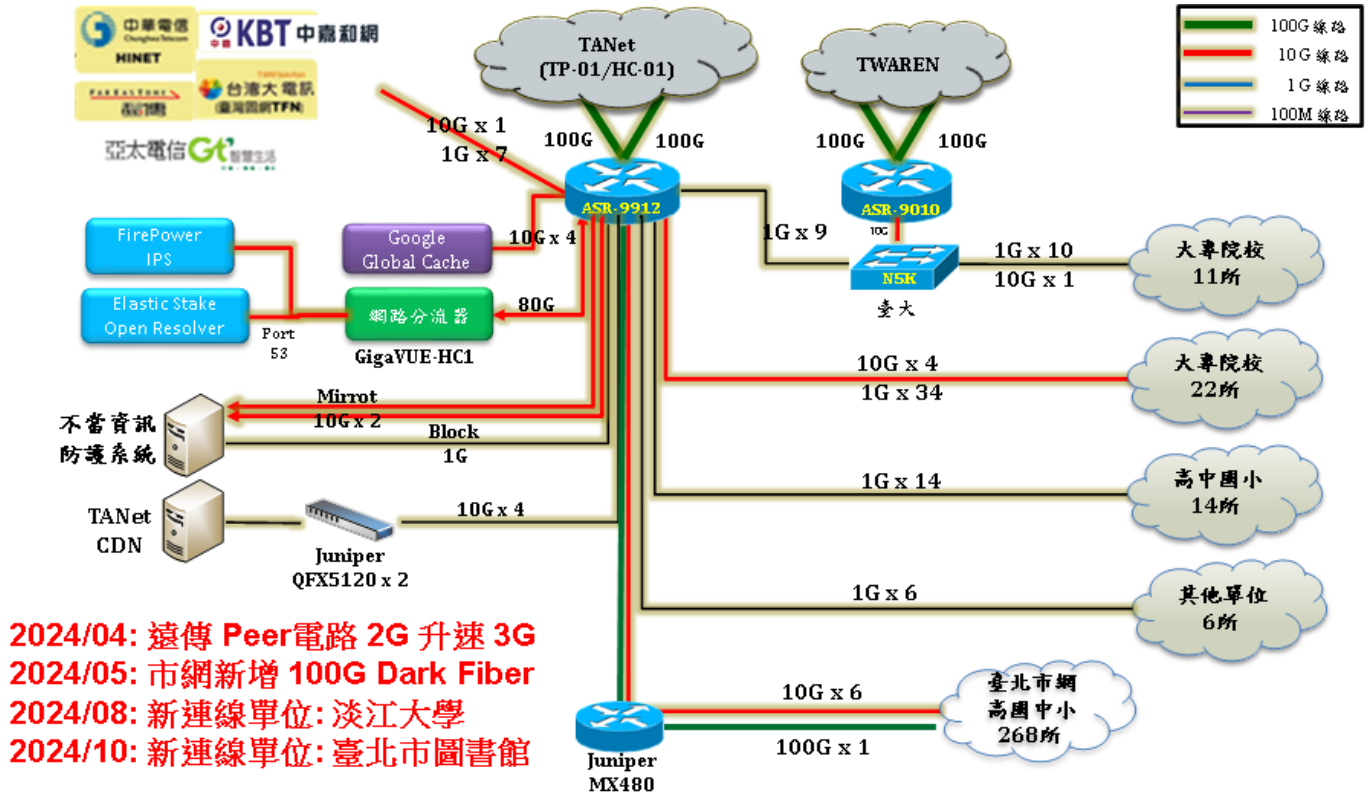
7.技術文件分享: 完成 3 份以上網路資安文件

8.使用區網連線學校基礎資料更新情況進行評核與審查: 每年至少完成 3 個單位評核與審查

附表 1：區網網路架構圖

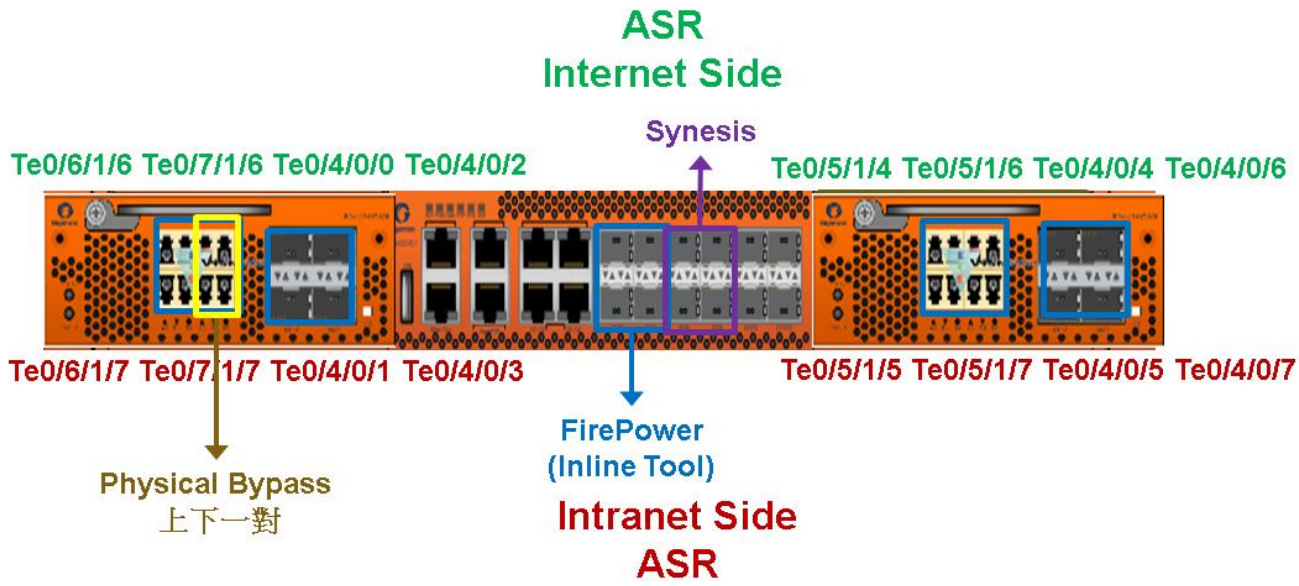
一、區網與連線單位(含縣(市)教育網路、連線學校、其他連線單位等)、TANet、

Internet(Peering)的總體架構圖

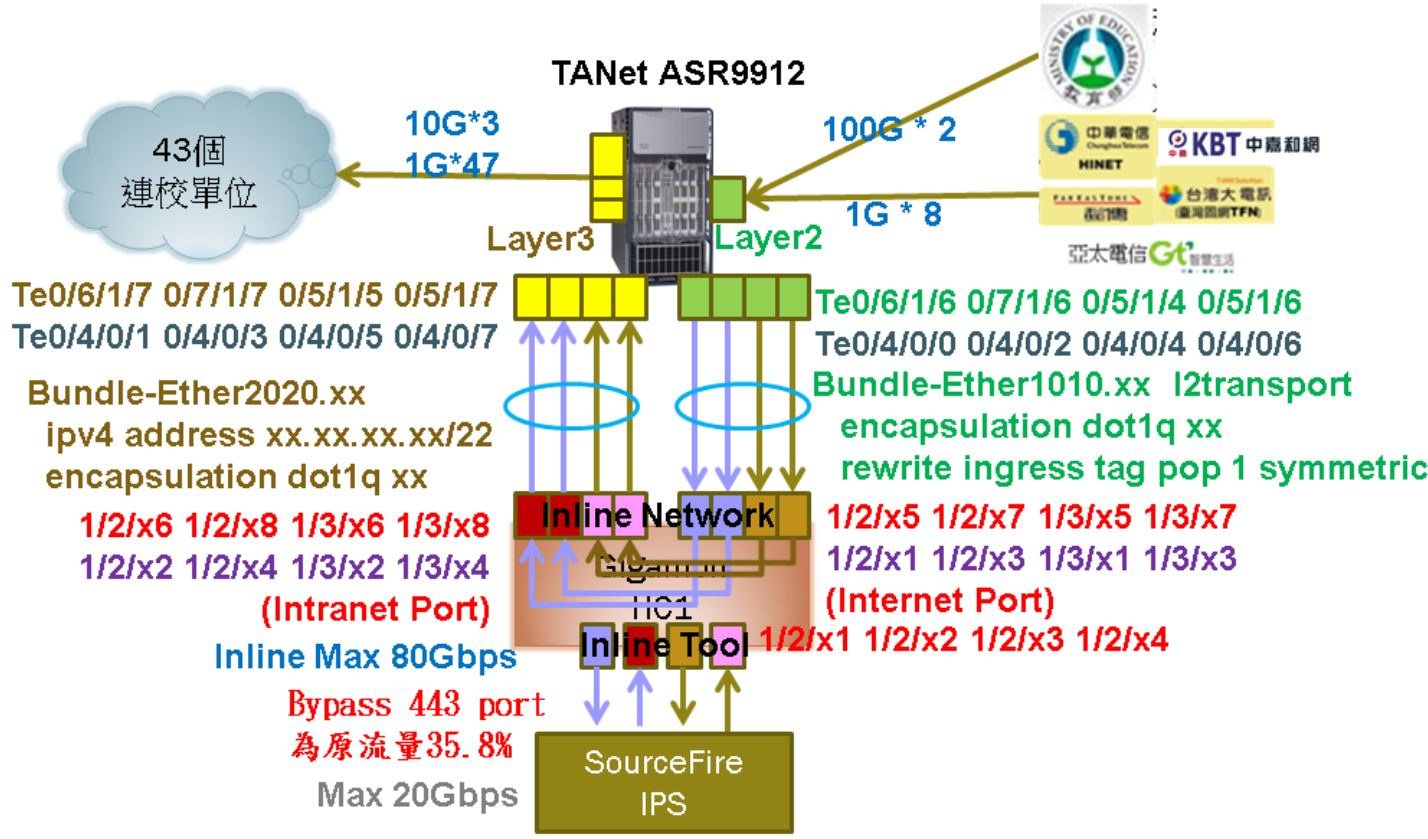


二、網路配合各種應用架構(如連線分流、頻寬管理)或資安架構(防火牆、IDS/IPS/WAF)的規劃或實際運作架構

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.	臺北市	20G	東豐	
	4.	臺北市	100G	中研院 Dark Fiber	
	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	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	2G	亞太 +中華	
	9.	國立臺北藝術大學	1G	中華	
	10.	國立臺北商業大學	1G	中華	
	11.	銘傳大學	1G	中華	
	12.	實踐大學	1G	中華	
	13.	臺北醫學大學	2G	台灣固網	台北校區 雙和校區
	14.	真理大學台北校區	1G	台灣固網	
	15.	大同大學	1G	遠傳電信	
	16.	龍華科技大學	1G	中華	
	17.	宏國德霖科技大學	1G	中華	
	18.	亞東技術學院	2G	遠傳電信	
	19.	致理科技大學	1G	中華	
	20.	黎明技術學院	1G	中華	
	21.	康寧大學	1G	中華	
	22.	華夏科技大學	1G	中華	
	23.	私立明志科技大學	1G	遠傳電信	

	24.	臺北海洋技術學院	2G	遠傳電信	
	25.	德明財經科技大學	1G	中華	
	26.	法鼓文理學院	1G	中華	
	27.	臺北市立大學	1G	臺灣智慧光網	
	28.	國防部軍事情報局軍事情報學校	1G	亞太	
	29.	臺北科技大學	0G	中華	
	30.	臺北基督學院	1G	台灣固網	
	31.	臺灣科技大學	20G	Dark Fiber	
	32.	東吳大學	2G	中華	城中校區 雙溪校區
	33.	淡江大學	4G	中華+遠傳	
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	中嘉和	
	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	1.	新北市立圖書館	1G	中華	

之連線單位(不含ISP)	2.	台北市立圖書館	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.	中央氣象署	1G	台智光(東豐)	
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.				