臺灣學術網路(TANet)區域網路中心
臺北區網 1

『106 年度基礎維運與資安人員計畫』

105　　年　　12　　月

【目　　錄】

壹、計畫基本項目

一、計畫期程

106 年 1 月 1 日至 106 年 12 月 31 日

二、計畫執行單位

臺北區域網路中心 1—臺灣大學計算機及資訊網路中心

貳、計畫執行內容

一、區域網路中心基本維運

(一)現況說明

1. 目前與北區區網直接介接的 ISP 包含了中華電信 3Gbps、遠傳電信 2Gbps、中嘉和網電信 1Gbps、亞太電信 1Gbps 及台灣固網 1Gbps。目前這些 ISP 都已接在新世代骨幹路由器上，提供連線學校使用。(附錄一 北區區網連線圖)
2. 台北市市網現今為 亞太電信 10Gbps、中華電信 1Gbps x 2。
3. 提供區網連線學校 IP 網段查詢。
4. 參與 TWAREN 骨幹網路設備維運計劃。
5. 對連線學校(單位) 提供 WEB 及 DNS 服務狀態連線偵測情形詳細紀錄。
6. 連線單位數：51 所學校/單位。
7. 尚可供所屬連線學校申請分配之 IP ：0 個。
8. 人力狀況
   - 單位主管：顏嗣鈞
   - 網管：游子興
   - 資安業務負責人：待聘
   - 編制內及約聘僱專職人員 8 名。

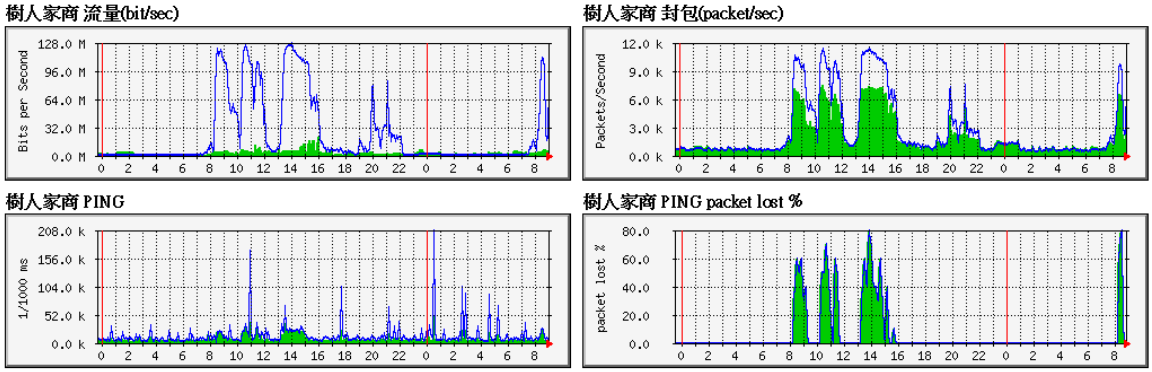
   協助處理各伺服器系統（WEB, FTP, DNS）之例行維護、問題諮詢及統計監控使用狀況，FreeBSD/Linux 伺服器系統維護、管理及統計使用者使用行為並翻譯編寫 FreeBSD 及 Linux 相關文件，網路流量分析、監控及資料庫建立等。
9. Router 線路異動與路由管理。
10. 設置故障雙向測試系統，縮短故障排除時間，並提供 ISP 業者之聯絡資訊。
11. 提供各連線學校自行修改單位資料之網頁界面。

12. 推動各連線學校資源交流 (例如網路電話、IPv6、網路管理經驗分享) 。
13. 每年暑假期間皆會固定舉辦網路技術之研討會。經由固定舉行研討會，期能將技術及網路科技與資訊安全等最新訊息達成全面性往下紮根，使區網連線之中小學能快速接收到最新資訊。
14. 迄今尚無無法連線學校。

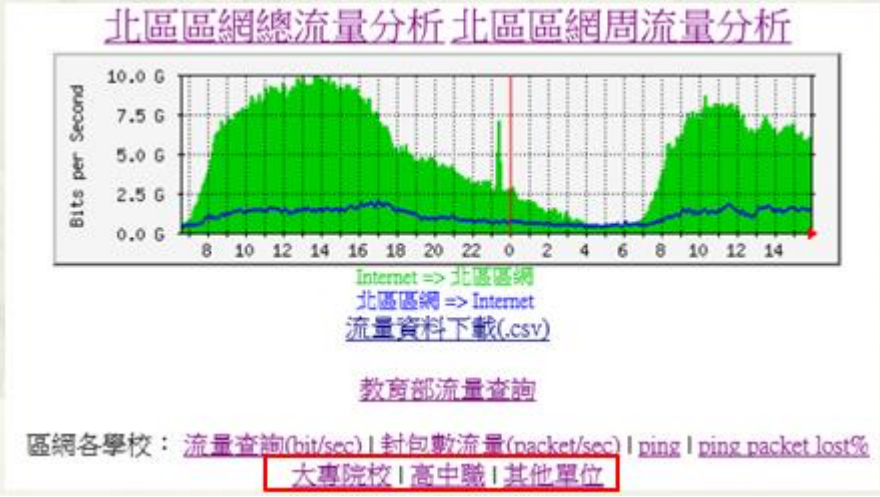
(二)工作內容

繼續維持日常優良服務並作下列推廣：

1. 推動各連線學校資源交流 (例如 IPv6 應用服務及 VoIP 網路節費電話推廣)。
2. 鑑於網站入侵高居不下的統計比例，設置網頁弱點掃描機制，提供有別於傳統系統弱點掃描未特別針對網站弱點的部份的稽核機制。
3. 協助調查大專院校及高中職連線單位網路設備支援 IPv6 之現況。
4. 統計並整理網路異常事件處理過程，分享解決網管相關經驗於區網會議，
   甲、 區網中心路由器佈線注意事項
   乙、 連線單位 peer ip 網段建議使用 /30 之網段
   丙、 Cache Server Solution
   丁、 備援線路
   戊、 Netflow Based 網路攻擊偵測系統
5. 將連線單位之流量、封包量、ping、packet lost% 整合顯示於一個畫面，可快速釐清網路異常問題。

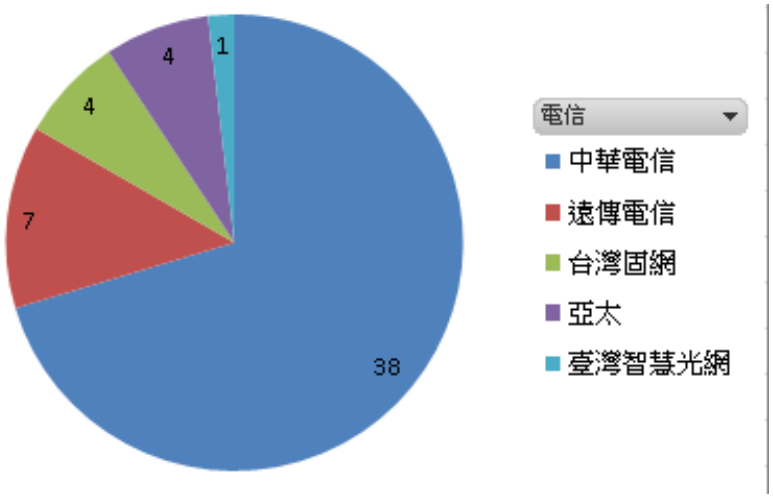


6. 將連線單位分類為大專院校、高中職、其他單位，更容易查找圖表資訊。



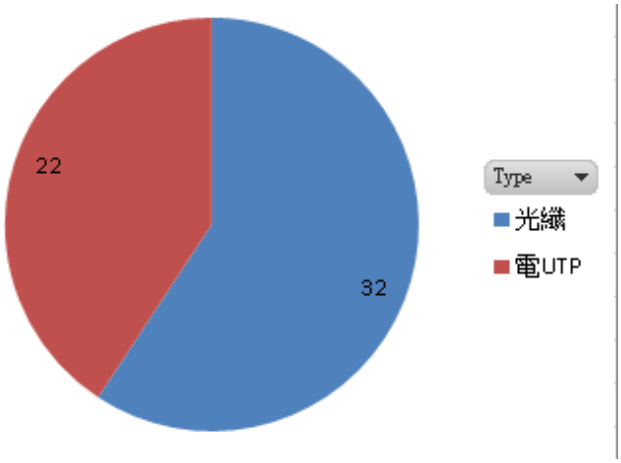
7. 使用 ELK Stack 記錄 TANET 區網 Router 之 Netflow 並提供 Src IP/Port、Dest IP/Port 等搜尋功能，並可依據封包數或流量查找 Top10 Src IP、Dest IP，若有網路異常流量發生，可快速釐清問題。
8. 使用 Cacti 收集 TANET 區網 Router Syslog 記錄並提供 Link Up/Down、Login Alerts 及 Config 指令修改通知。
9. 連線品質管理，使用 Ping Latency 監控 Yahoo/Google/Facebook/Hinet DNS 等常見之入口網站與服務。
10. ISP 線路統計

列標籤	計數 - 電信
中華電信	38
遠傳電信	7
台灣固網	4
亞太	4
臺灣智慧光網	1
總計	**54**



11. 線路介面型態統計

列標籤	計數 - Type
光纖	32
電UTP	22
總計	54



(三)創新服務

1. 建構即時且自動化之網路品質監控系統，改善傳統被動式網路異常通知，建構化被動為主動之網路品質監控系統

2. 建立主動網路偵測機制: 使用者端

甲、提供網路速度測試工具: 網頁測速、Android/iPhone Speed Test App

乙、網路簡易偵測工具: Ping Latency、Traceroute 出口路徑查詢

3. 建立主動網路偵測機制: 網路設備端

甲、連線介面偵測: 頻寬使用狀況

乙、網路設備偵測: Ping Latency、CPU 使用率

丙、伺服器偵測: CPU 使用率、記憶體使用率、硬碟使用率

4. IP 全球地址資料庫查詢 (附錄二)

甲、用途:

i. 國際頻寬使用率分析: 國家/地區/ISP/AS#

ii. 帳號盜用分析: VPN 帳號登入 IP 地點分析

iii. 駭客攻擊來源分析

乙、購買 IP2Location 商業版本(USD$649)，資料庫已更新至最新版本 2016/11

版本	更新年/月	網段筆數
免費版	2015/10	2,178,274
商業版	2015/10	12,857,322
商業版	2016/11	13,007,878

5. 區網連外架構圖 (附錄三)

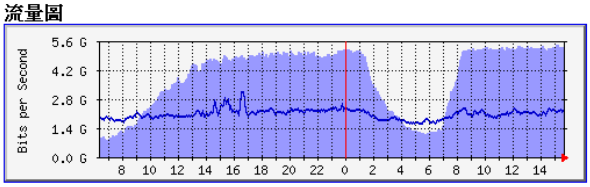
甲、圖示化顯示區網出口節點，可點選出口節點顯示對應 peering ip

乙、整合顯示網路節點監測圖: 流量圖、Ping、Packet Lost%

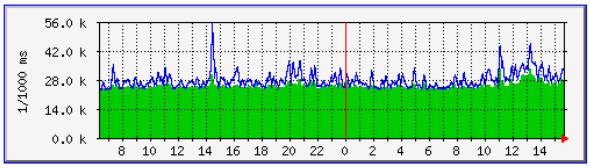
教育部-TWGATE國際頻寬

Peer IP: 175.41.61.45

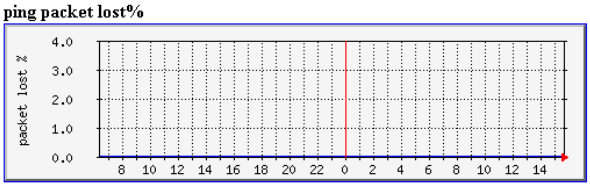
流量圖



PING RTT



ping packet lost%



6. Traceroute 路徑查詢 (附錄四)

甲、依據輸入 ip 或 host 可動態顯示出口路徑

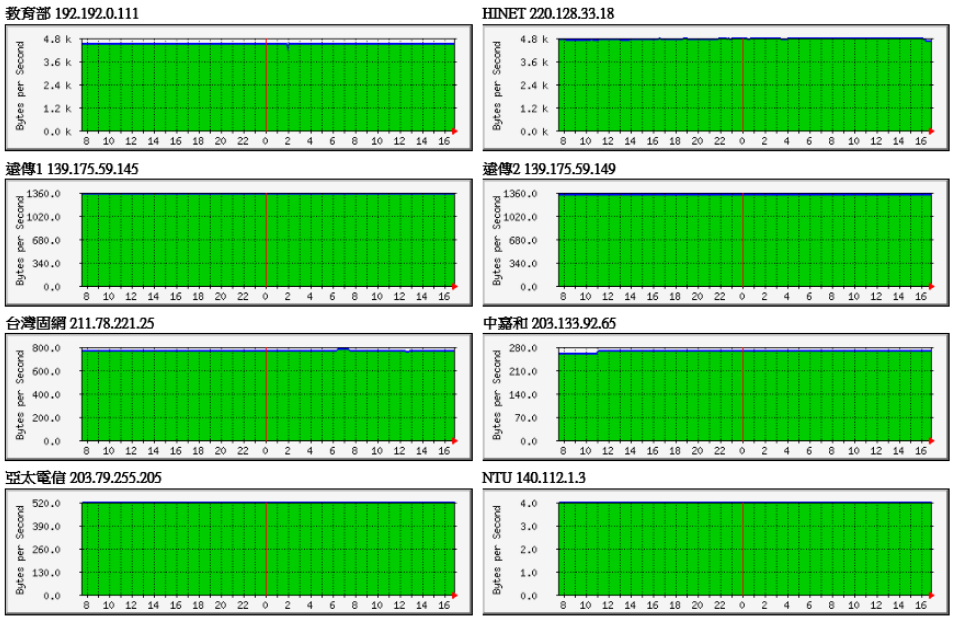
乙、即時出口路徑之網路品質監測圖顯示: 流量圖、Ping、Packet Lost%

丙、整合 IP 地址資料庫+ 封包經過路徑顯示於 Google Map

7. BGP Neighbor Accepted Prefix

甲、針對 5 家 ISP peering，監控 BGP Prefix 筆數之變化。

BGP Neighbor Accepted Prefix

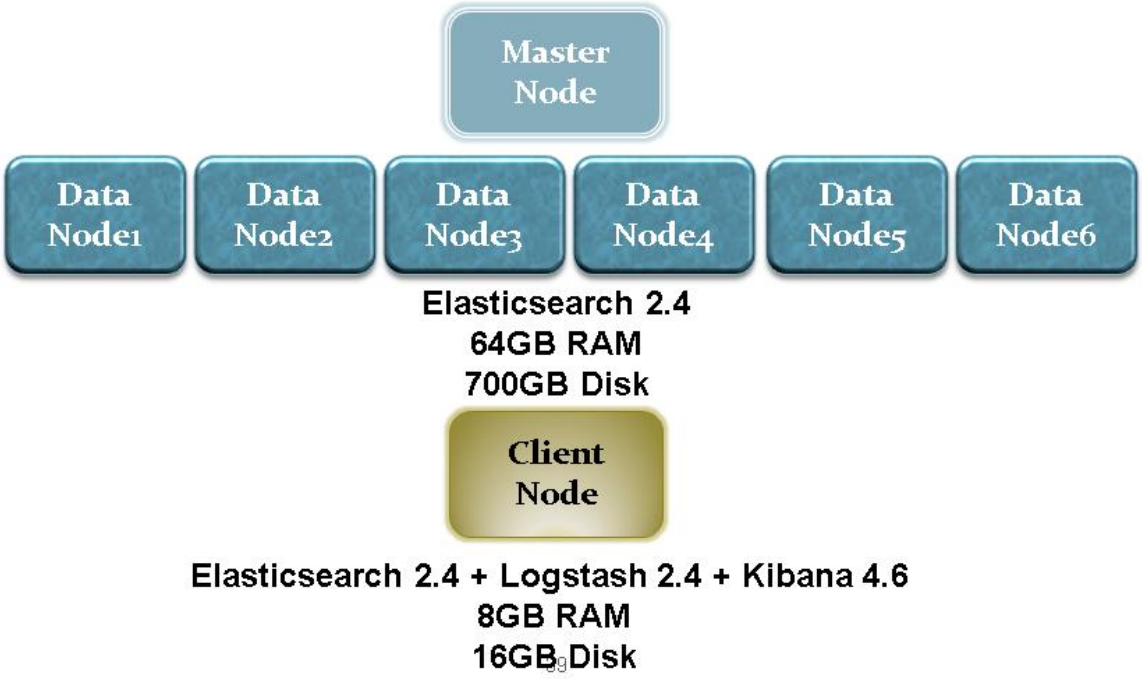


8. Netflow Based 網路攻擊偵測系統

甲、 DDoS 攻擊發生後，需要快速分析攻擊來源與型態，才能進行阻斷或緩解，台大區網使用 Big Data 分析工具: ELK Stack

乙、 ELK Stack，由三套工具所組成。Elasticsearch、Logstash、Kibana，Elasticsearch 負責資料之儲存，Logstash 負責收集各種格式之資料，Kibana 負責各種圖表之呈現。

丙、 分析方法使用路由器導出 Netflow 流量資料，並用如下之架構圖進行資料分析與呈現，共使用 8 台虛擬機，其中一台 Master Node 負責管理資料，六台 Data Node 負責儲存與處理資料，一台 Client Node 負責接收與圖表資料呈現。



(四)工作目標

1. 定期召開管理委員會等並提供相關會議資料及下載。
2. 提供連線單位網路相關諮詢服務。
3. 持續提供穩定不斷線之優質服務為本區網中心工作目標。
4. 提供各式網路備援方案以提升各連線單位之網路可用率。
5. 網路品質監控預計全面導入 Cacti 監控系統，並於網管會議或暑期教育訓練課程中分享建置經驗。
6. 針對連線單位 DNS Server 若使用版本過於老舊，將輔導升級或直接安裝新版本，預計於網管會議與暑期教育訓練課程進行宣導。
7. 為節省電力資源與有效運用電腦資源，建構區網雲端虛擬伺服器:

   甲、區網網頁備份主機

   乙、網路品質偵測主機

   i. 線路品質偵測

   ii. Netflow 記錄與搜尋

   iii. Syslog 記錄與 Alert 通知

   丙、區網連線學校測試主機

   i. 可綁定連線學校提供特定網段 IP，做連線測試，可快速釐清為 Source IP 或電路問題

   ii. 提供 JPerf 測速 Server 主機服務
8. 持續整理網路異常事件處理過程，針對異常狀況擬定處理對策 SOP，並在區網會議提供經驗分享。
9. 針對目前尚未使用 ipv6 之連線單位，主動聯繫並輔導協助其上線，若是設備老舊不支援，則提供 Open Source Router 軟體例如 pfsense，提供技術支援與相關設定範本。
10. 針對第二期能源國家型科技計畫-節能主軸中心-校園節能，繼續推廣高國中小之學校資訊設備，能由實體主機轉換為雲端虛擬主機。

(五)預期效益

1. 舉辦 6 場以上網路科技、資安技術及智慧財產權、個人資料保護作業施行等相關議題之教育訓練，以提升連線學校與本校教職員處理相關問題的能力。
2. 提升網路效率及其附加價值，例如：推動連線學校網路電話的普及率，建立網路通訊平臺，以節省國家經費。
3. 為有效推動 IPv6，完成 IPv6 測試網站與 IPv6 DNS 反解服務，區網提供之伺服器 100% 皆有 IPv6 之網址與 IPv6 DNS 反解位址。
4. 協助連線學校網路應用頻寬管理、P2P 網路應用管理及網路應用分析，預計達成連線學校授與服務數之 100%。
5. 透過網路品質偵測系統提供網路異常訊息，可即時通知連線學校網管相關人員，有此需求之連線學校預計 80%皆可提供此服務。
6. 依據區網 Router 提供之 Netflow 記錄，可提供各時段之 ip 連線記錄，並可加快網路發生異常後之處理速度,預計所有區網對外連線 100%皆啟用 Netflow 記錄。
7. 針對 Netflow 記錄進行即時監控，及早發現網路異常活動，可確保網路頻寬有效被運用。
8. 推廣雲端節能計畫，預計再提供 50 組虛擬主機，將高國中小之學校資訊設備轉換為雲端虛擬主機。
9. IP 全球地址資料庫之應用實例：帳號盜用分析、網路頻寬使用分析等。

(六)辦理資訊推廣活動

場次	研習課程	上課地點	研習時數	人數
10501	雲端技術簡介	計中 106 室	3 小時	100
10502	網路設備基礎管理	計中 106 室	3 小時	100
10503	惡意程式查找入門	計中 106 室	3 小時	100
10504	駭客攻擊手法：APT 攻擊&勒索軟體介紹	計中 106 室	3 小時	100
10505	程式設計實務課程：Android/ iPhone	計中 212 室	6 小時	50

10506	DNS Server 架設與升級	計中 212 室	6 小時	50
10507	pFsense 防火牆架設與設定	計中 212 室	6 小時	50

二、建構區網中心、連線單位及學校資通安全基本防護

(一)工作內容

1. 連線學校接獲「教育機構資安通報平台」發送的資安通報或警訊後，必須於限期內完成異常主機之惡意程式查找與清除，網管人員手動查找既無效率又缺乏說服力。現提供連線學校提供異常主機惡意程式查找手冊，使用微軟免費提供的檢測工具，將主機之程序、網路連線與封包等做完整的查找，找出主機中之惡意程式。
2. 因應個資法的實施，各校對於自己是否會無意中於網站洩漏個資而感到憂心，手動檢查也怕有所遺漏且浪費時間。現提供連線學校提供網站防洩漏個資偵測服務，使用掃描平台檢測目標網站，並將可能洩漏的風險輸出報告提供給使用者作為修正佐證。
3. 鑑於連線學校的網站多半為數位老師交接完成或架設已久從未檢查更新，常導致網站暴露許多可被利用的弱點，導致使用者會因為瀏覽網頁受害。現提供連線學校提供網站弱點掃描服務，使用掃描平台檢測目標網站，並將存在的弱點及可能產生的攻擊輸出報告提供給使用者作為修正佐證。
4. 由於區網底下連線學校眾多，各校也會自行架設 DNS server 提供服務，但因對設定不熟悉，便很容易成為公開的 DNS server 導致被利用來進行攻擊。現提供連線學校提供 DNS server 檢測，針對 Recursion、Transfer 及反解-完整性做檢查，並提供修正說明讓管理者可以依序操作修正設定。

(二)預期效益

1. 協助連線學校異常主機查找惡意程式，預計達成連線學校授與服務數之 100%。
2. 協助連線學校偵測是否於網站洩漏個資，預計達成連線學校授與服務數之 100%。
3. 協助連線學校偵測是否網站有弱點，預計達成連線學校授與服務數之 100%。
4. 協助連線學校偵測 DNS server 是否設定正確，預計達成連線學校諮詢數之 100%。

參、經費需求

申請單位: 國立臺灣大學	計畫名稱：臺灣學術網路(TANet)區域網路中心 106 年度基礎維運與資安人員計畫
計畫期程： 106 年 1 月 1 日至 106 年 12 月 31 日	
計畫經費總額：**1,580,000** 元，申請金額：**1,580,000** 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：	

8 經費項目		計畫經費明細				**教育部核定計畫經費（申請單位請勿填寫）**	
		單價（元）	數量	總價(元)	說明	金額（元）	說明
一、人事費	專任行政助理薪資(網管)	31,520	2	63,040	1.薪資預算含年終獎金 1.5 個月。 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 106 年 3 月 1 日提敘一級。		
		32,240	11.5	370,760			
	行政助理勞、健保費(網管)	3822	2	7,644			
		4002	10	40,020			
	行政助理勞退公提(網管)	1,908	2	3,816			
		1,998	10	19,980			
	二代健保補充保費(網管)	924	1	924	年終獎金 1.91%之二代健保補充保費。		
	專任行政助理薪資(資安)	43,570	13.5	588,195	1.薪資預算含年終獎金 1.5 個月。 2.勞健保、勞退費用依勞基法規定辦理。 3.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。		
	行政助理勞、健保費(資安)	5,275	12	63,300			
	行政助理勞退公提(資安)	2,634	12	31,608			

申請單位: 國立臺灣大學		計畫名稱：臺灣學術網路(TANet)區域網路中心 106 年度基礎維運與資安人員計畫					
計畫期程： 106 年 1 月 1 日至 106 年 12 月 31 日							
計畫經費總額：**1,580,000** 元，申請金額：**1,580,000** 元							
	二代健保補充保費(資安)	1,248	1	1,248	年終獎金 1.91%之二代健保補充保費。		
			小計	**1,190,535**			
二、業務費	講座鐘點費	1,600	30	48,000	外聘 1,600，1 場 3 小時。預計舉辦 10 場，共 48,000 元。		
	講座鐘點費補充保費	917	1	917	依二代健保規定，講座鐘點費共 48,000 元，須 1.91%補充保費 917 元。		
	工讀費	133	600	79,800	因應資安行政助理職缺若未如期徵補、及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)，每月約 50 小時。 3、依本校臨時人員薪資規範支給。		
	工讀費補充保費	1,524	1	1,524	依二代健保規定，工讀費共 79,800 元，須 1.91%補充保費 1,524 元。		
	國內旅費、運費	1,500	10	15,000	參加會議校內同仁或來訪學者專家、講師之旅、運費、停車費，單程以 1,500 元估算，預估 10 人次來回為 1,500*10=15,000 元		

申請單位: 國立臺灣大學	計畫名稱：臺灣學術網路(TANet)區域網路中心 106 年度基礎維運與資安人員計畫						
計畫期程： 106 年 1 月 1 日至 106 年 12 月 31 日							
計畫經費總額：**1,580,000** 元，申請金額：**1,580,000** 元							
	膳宿費	1,600	4	6,400	外出參與會議之住宿費，預估為 4 人次。1,600*4=6,400 元		
		100	300	30,000	辦理研習會、座談會或訓練進修，預估 6 場，每場 50 人次。(誤餐費 80+茶點費 20)		
	維護運作：辦公室電信費、水費、電費	1,000	12	12,000	處理區網事務及回覆 TACERT 資安事件通訊費用，月租費 1000 元*12 個月。		
	設備維護費	700	12	8,400	區網中心相關主機等維護費，預計每月約 700 元*12 個月，以 8,400 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	12,000	1	12,000	區網中心設備維護費及其他網路運作相關網路資訊材料		
	專業證照、教育訓練費	30,000	1	30,000	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	15,424	1	15,424	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。		
			小計	**319,465**			

申請單位: 國立臺灣大學				計畫名稱：臺灣學術網路(TANet)區域網路中心 106 年度基礎維運與資安人員計畫			
計畫期程： 106 年 1 月 1 日至 106 年 12 月 31 日							
計畫經費總額：**1,580,000** 元，申請金額：**1,580,000** 元							
三、設備及投資	設備費	70,000	1	70,000	電腦、網路、伺服器、交換器...等資訊設備(單價 1 萬元以上且耐用年限超過 2 年)		
	小計			**70,000**			
合 計				**1,580,000**			
承辦單位		會計單位		機關長官或負責人	教育部承辦人	教育部單位主管	

備註：

1、依行政院 91 年 5 月 29 日院授主忠字第 091003820 號函頒對民間團體捐助之規定，為避免民間團體以同一事由或活動向多機關申請捐助，造成重複情形，各機關訂定捐助規範時，應明定以同一事由或活動向多機關提出申請捐助，應列明全部經費內容，及擬向各機關申請補助經費項目及金額。

2、補助案件除因特殊需要並經本部同意者外，以不補助人事費為原則；另內部場地使用費及行政管理費則一律不予補助。

3、各經費項目，除依相關規定無法區分者外，以人事費、業務費、雜支、設備及投資四項為編列原則。

4、雜支最高以【(業務費)*5%】編列。

補助方式：

補助方式：

□全額補助

□部分補助【補助比 %】

□酌予補助

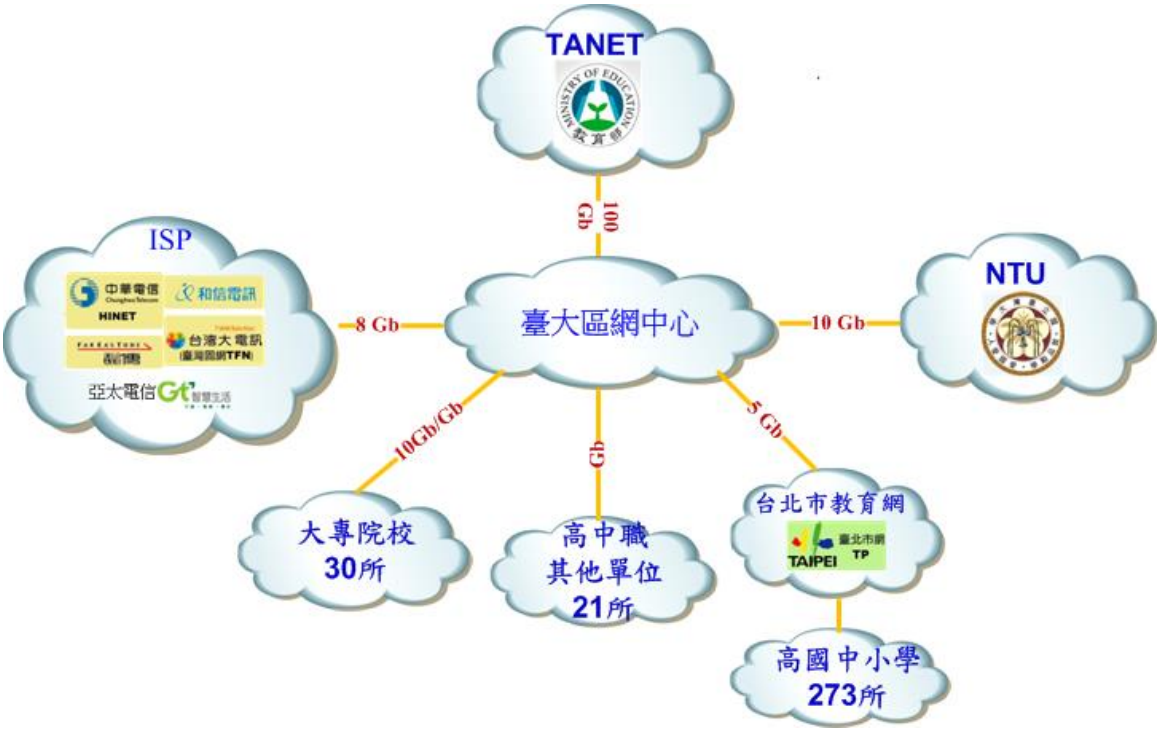
餘款繳回方式：

□繳回 （請敘明依據）

□不繳回（請敘明依據）

□其他（請備註說明）

附錄一、台北區網連線架構圖



附錄二、IP 全球地址資料庫查詢

IP 地址資料庫查詢

IP 地址資料庫: ip2location

host or ip: www.teamviewer.com

驗證碼： 19406 19406 送出

IP 全球地址資料庫查詢結果:

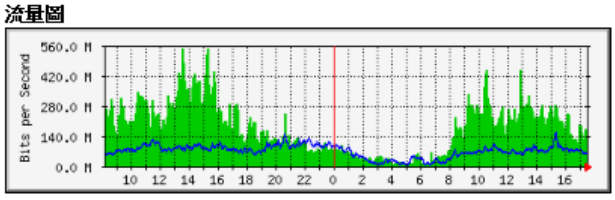
IP 全球地址資料庫: ip2location

ip	Country Code	Country Name	City	Latitude	Longitude	ISP	Domain
46.163.100.220	DE	Germany	Koeln	50.93333	6.95	Host Europe GmbH	hosteurope.de

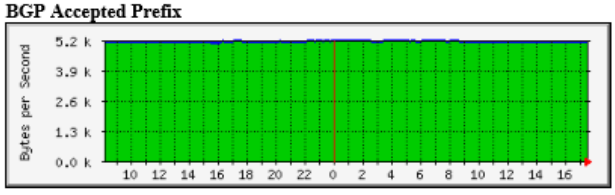
附錄三、區網出口路徑拓樸圖

HINET_PEER1

流量圖

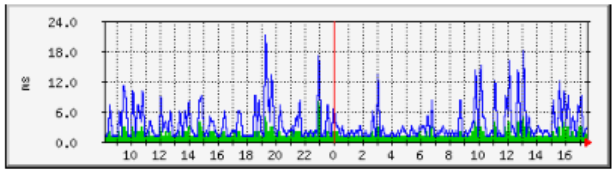


BGP Accepted Prefix

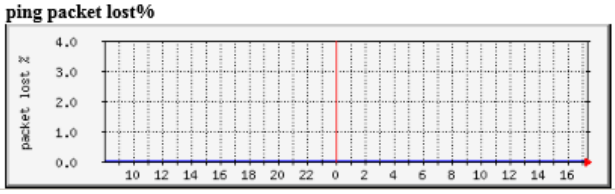


Peer IP: 211.20.43.62

PING RTT



ping packet lost%



附錄四、Traceroute 出口路徑查詢

Traceroute 出口路徑查詢

host or ip: www.facebook.com

驗證碼： 87775 送出

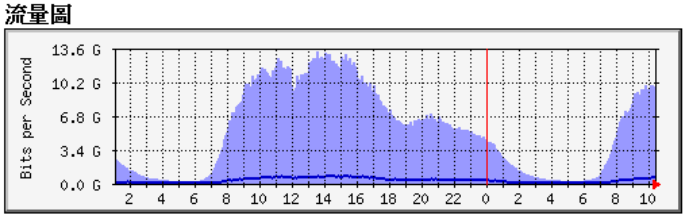
※ip2location version: 2016/11

Traceroute www.facebook.com 出口路徑查詢結果

Seq	hostname	ip	responsetimes1	responsetimes2	responsetimes3	router	country	city	latitude	longitude	ISP	Domain
1	163.28.16.254	163.28.16.254	0.765	0.775	0.816	台大區網 Router6509	TW	Taipei	25.04776	121.53185	MOEC	moec.gov.cy
2	192.192.61.82	192.192.61.82	1.819	1.574	1.791	臺北主節點	TW	Taipei	25.04776	121.53185	MOEC	moec.gov.cy
3	192.192.61.73	192.192.61.73	1.715	1.872	1.856	教育部-TP-ISP	TW	Taipei	25.04776	121.53185	MOEC	moec.gov.cy
4	203-163-222-13-static.tpix.net.tw	203.163.222.13	2.389	2.447	2.43	TPIX台北網際網路交換中心	TW	Taipei	25.04776	121.53185	Chief Telecom Inc.	chief.com.tw
5	po101.psw01c.tpe1.tfbnw.net	31.13.31.61	1.752	1.741	1.724		TW	Taipei	25.04776	121.53185	Facebook Ireland Ltd	facebook.com
6	173.252.67.17	173.252.67.17	1.714	1.728	1.634		NL	Amsterdam	52.37403	4.88969	Facebook Inc.	facebook.com
7	edge-star-mini-shv-01-tpe1.facebook.com	31.13.87.36	1.756	1.739	1.734		TW	Taipei	25.04776	121.53185	Facebook Ireland Ltd	facebook.com

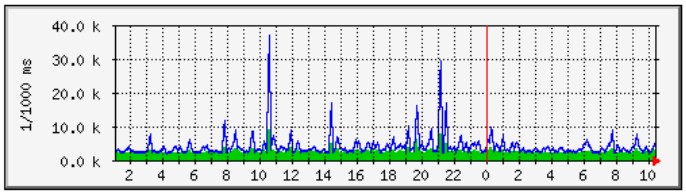
TPIX台北網際網路交換中心

流量圖



Peer IP: 203.163.222.13

PING RTT



ping packet lost%