113年度臺北區網I
年度報告

- 單位：國立臺灣大學
- 計資中心主任：周承復教授
- 網路組組長：謝宏昀教授
- 報告人：游子興、史詩妤

大綱

* 1.經費與人力
* 2.網路管理
* 3.資安服務
* 4.特色服務
* 5.成效精進
* 6.基礎維運
* 7.連線學校服務
* 8.未來營運與建議

1.1 區網經費

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)

* 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%

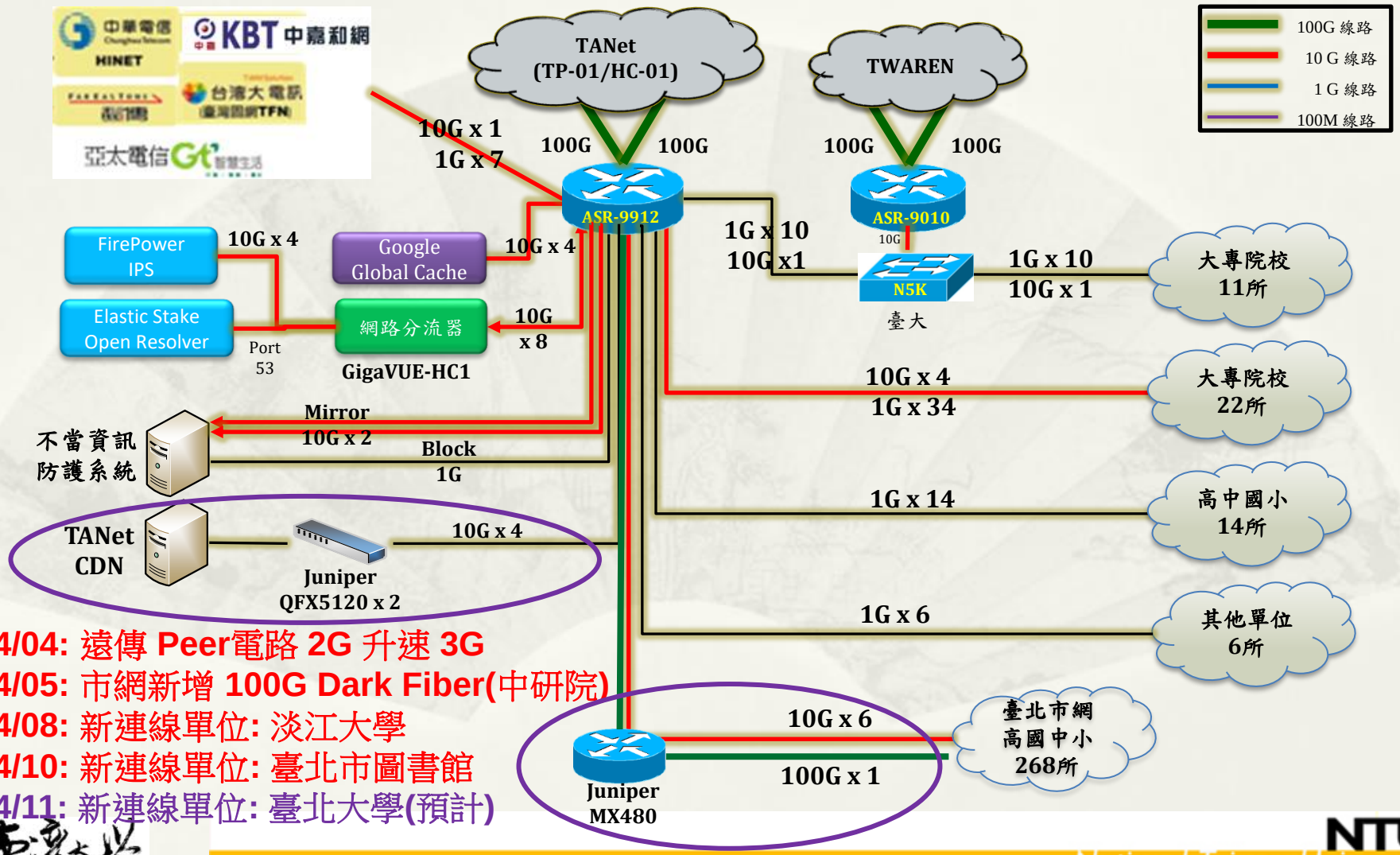
1.2 區網人力

* 計資中心主任：周承復教授
  * E-mail：ccf@csie.ntu.edu.tw
  * 電話：(02) 33665001
* 網路組組長：謝宏昀教授
* 網管負責人：游子興
  * E-mail：davisyou@ntu.edu.tw
  * 電話：(02) 33665008
* 資安負責人：史詩妤
  * E-mail：judyshih@ntu.edu.tw
  * 電話：(02) 3366513
* 編制內專職及約聘僱人員8名

2.網路管理

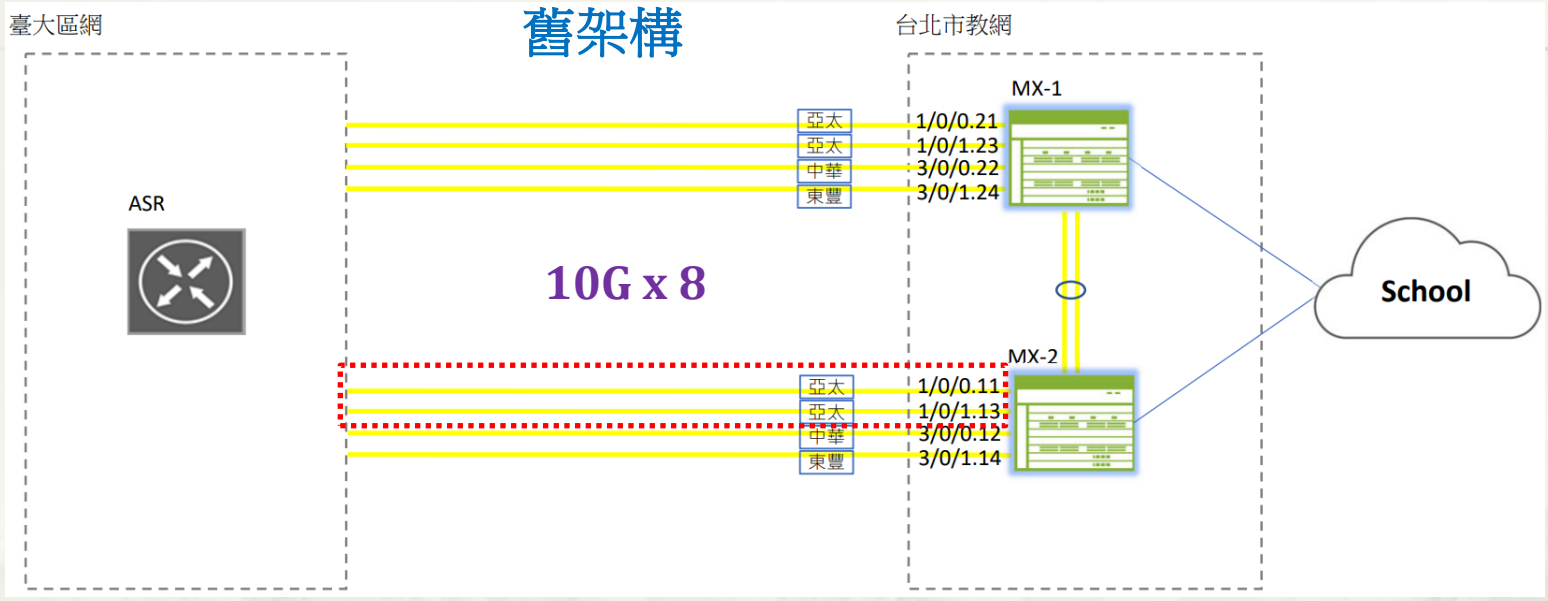
- 網路架構
- 歷年網路流量比較
- 連線單位 IPv6 完成率

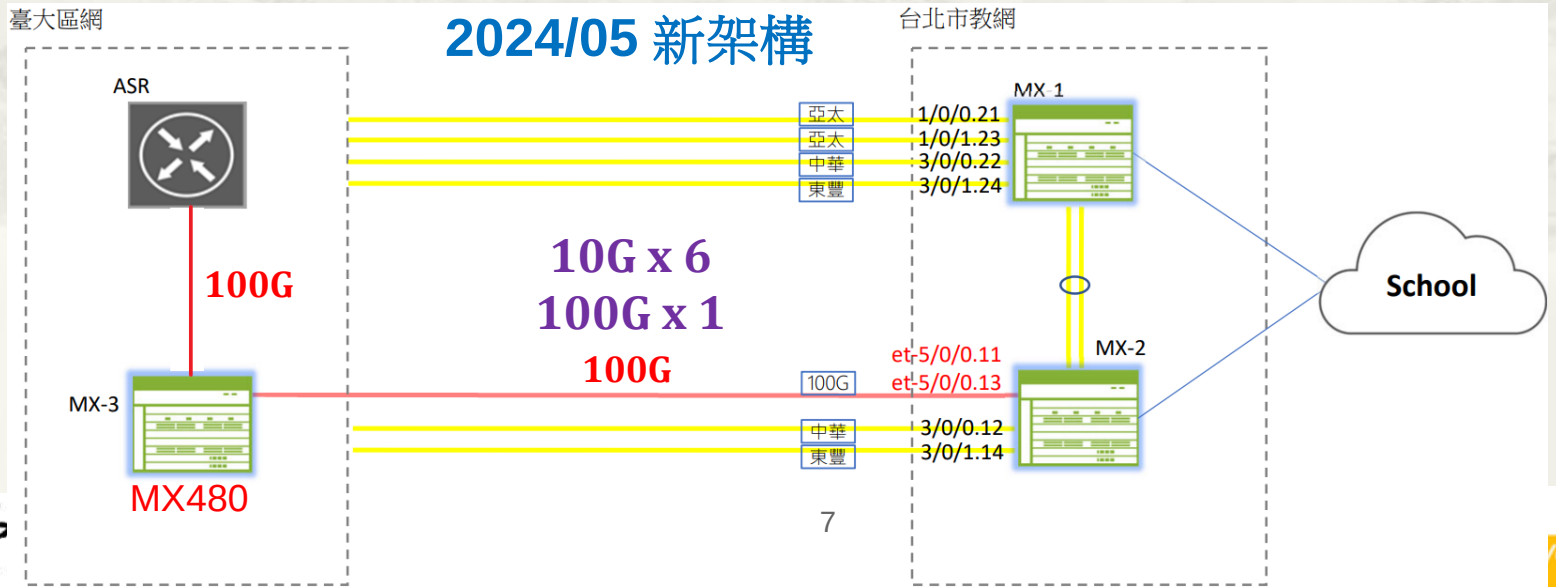
台北區網 I 網路架構



2024/04: 遠傳 Peer電路 2G 升速 3G
2024/05: 市網新增 100G Dark Fiber(中研院)
2024/08: 新連線單位: 淡江大學
2024/10: 新連線單位: 臺北市圖書館
2024/11: 新連線單位: 臺北大學(預計)

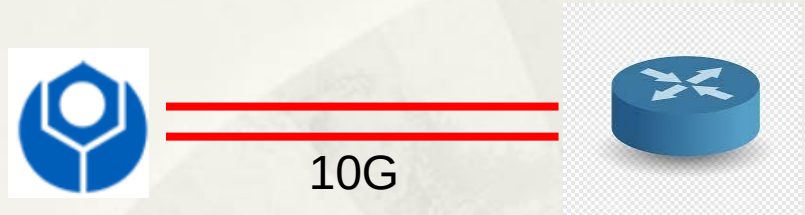
市網新增 100G Dark Fiber



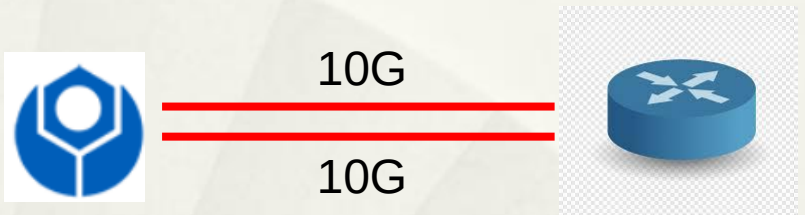


連線學校: 臺科大
2 蕊暗光纖頻寬擴增 10G x 2

舊架構

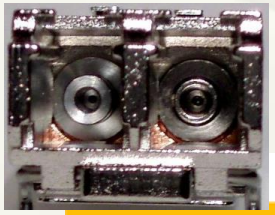


新架構



* 10G SFP+ 通用/一般

* 需要一對光纖傳輸



* 單蕊雙向BIDI光模組

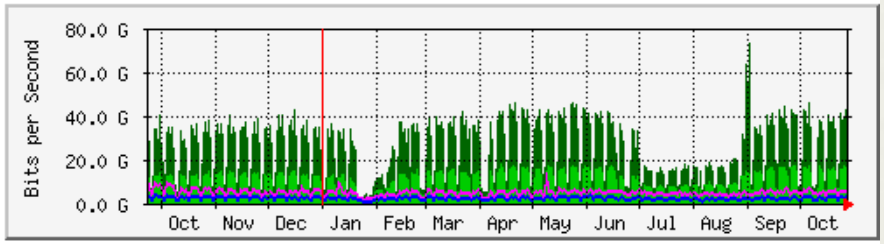
DWDM Passive
單蕊暗光纖 10G x 8

* 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

2024 網路流量比較

IPv4 流量

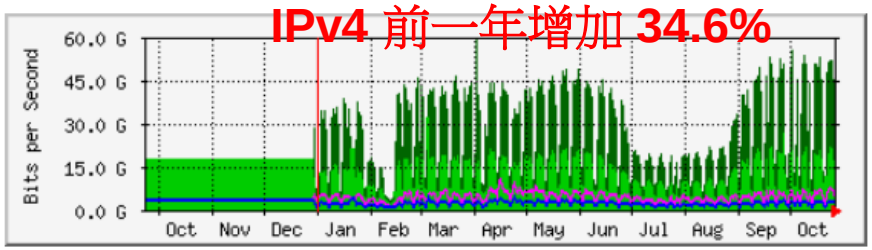
`Yearly' Graph (1 Day Average) 2023



	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%)

`Yearly' Graph (1 Day Average) 2024

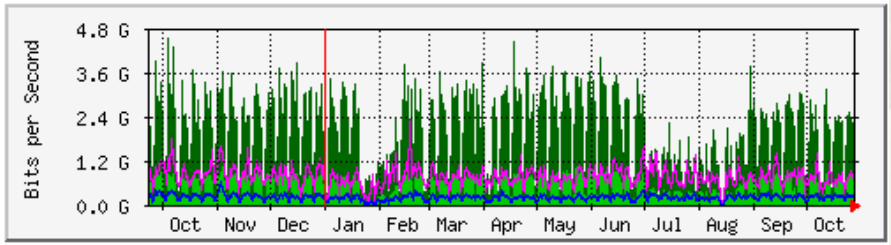
IPv4 前一年增加 34.6%



	Max	Average	Current
台北主節點 => 北區區網	59.6 Gb/s (59.6%)	13.6 Gb/s (13.6%)	7296.0 Mb/s (7.3%)
北區區網 => 台北主節點	10.6 Gb/s (10.6%)	2271.0 Mb/s (2.3%)	1393.2 Mb/s (1.4%)

IPv6 流量

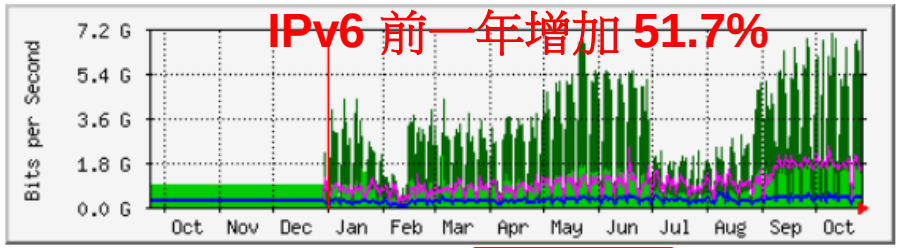
`Yearly' Graph (1 Day Average) 2023



	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%)

`Yearly' Graph (1 Day Average) 2024

IPv6 前一年增加 51.7%

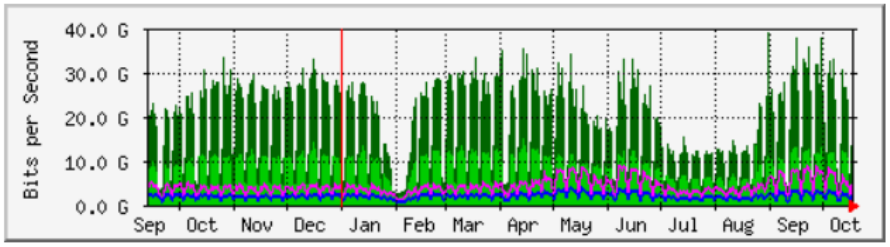


	Max	Average	Current
台北主節點 => 北區區網	7020.5 Mb/s (7.0%)	783.3 Mb/s (0.8%)	375.2 Mb/s (0.4%)
北區區網 => 台北主節點	2399.8 Mb/s (2.4%)	242.8 Mb/s (0.2%)	277.9 Mb/s (0.3%)

2023 網路流量比較

IPv4 流量

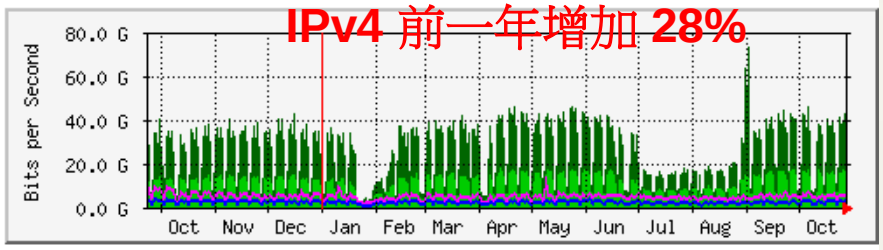
`Yearly' Graph (1 Day Average) 2022



	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

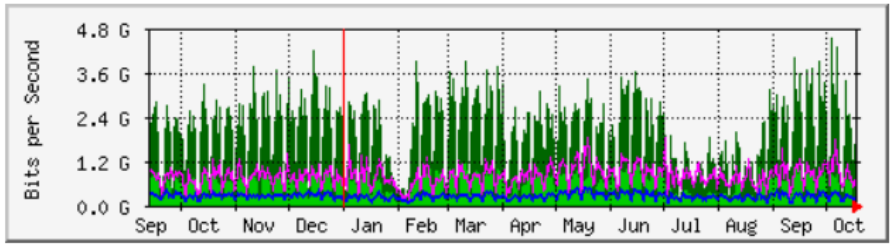
IPv4 前一年增加 28%



	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

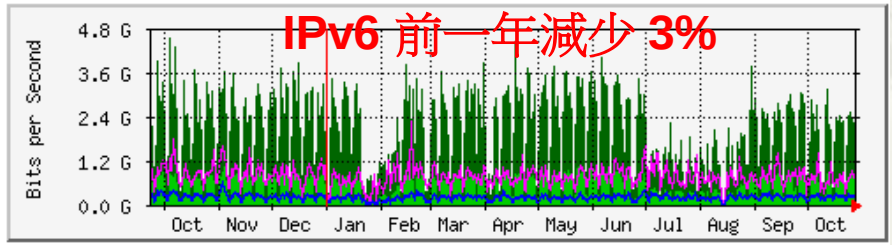
`Yearly' Graph (1 Day Average) 2022



	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

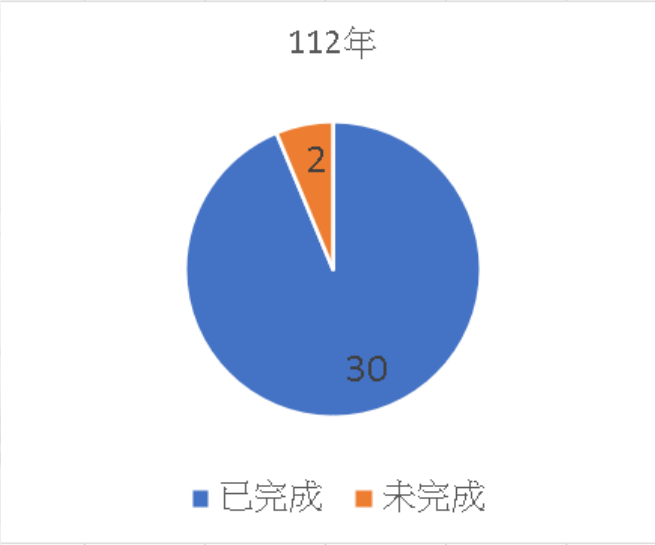
IPv6 前一年減少 3%



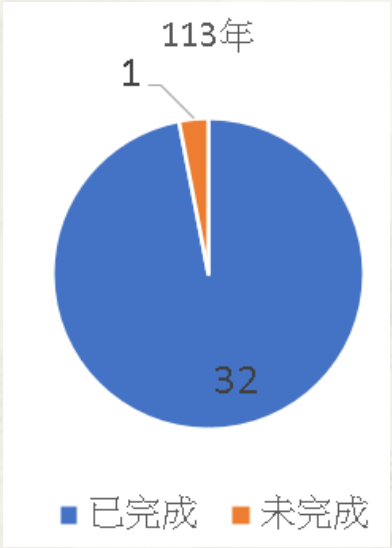
	Max	Average	Current
台北主節點 => 北區區網	4541.2 Mb/s (4.5%)	516.2 Mb/s (0.5%)	681.2 Mb/s (0.7%)
北區區網 => 台北主節點	2242.3 Mb/s (2.2%)	182.9 Mb/s (0.2%)	224.6 Mb/s (0.2%)

IPv6 大專院校完成率

* 路由網段設定完成率
  * 大專院校:33 間



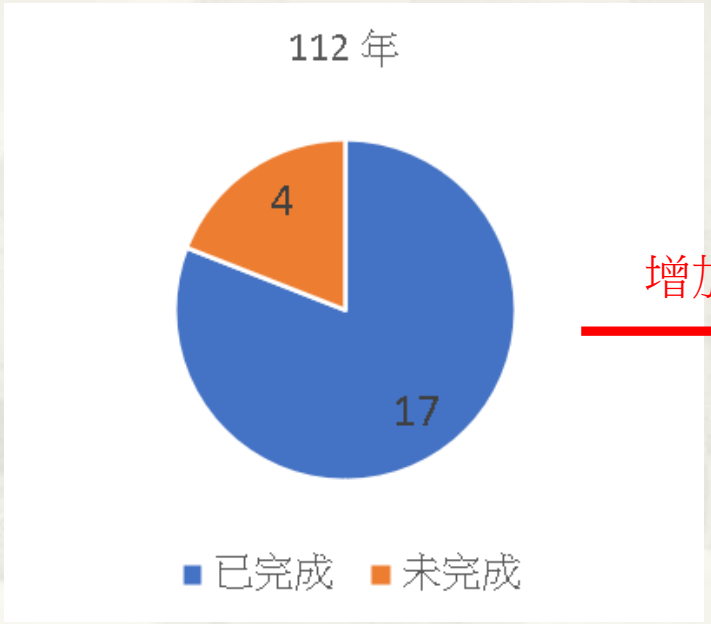
增加一間



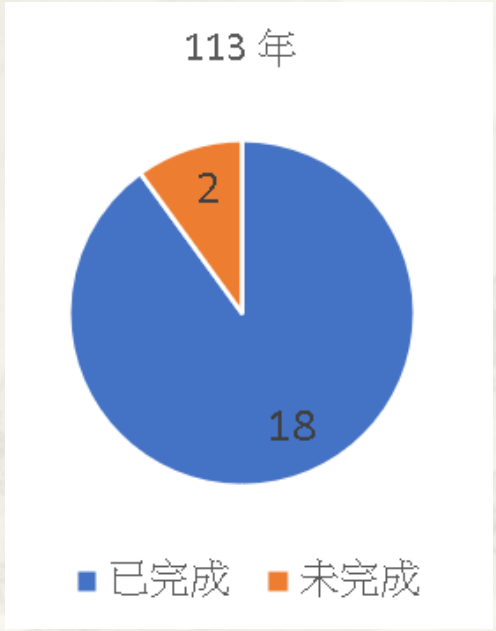
僅剩: 軍事情報局學校

IPv6 高國中小及其他單位完成率

* 路由網段設定完成率
  * 高國中小及其他單位: 20間



增加 2 間



僅剩: 中華民國學生棒球運動聯盟、國家地震中心

3.資安服務
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%

3. 資安服務
連線學校

* 資安事件通報
  * 連線單位自行通報資詢
  * 提供處理協助
  * 因人事調動，協助連線單位修改資安聯絡人
* 弱掃平台使用
  * 定期確認平台中未複測的中高風險網站，並通知該單位處理
* 威脅清單
  * 提供威脅清單給連線單位
* 與ASOC合作定期尋找學網內的威脅
  * 每月提供學網曝顯清單

4. 特色服務

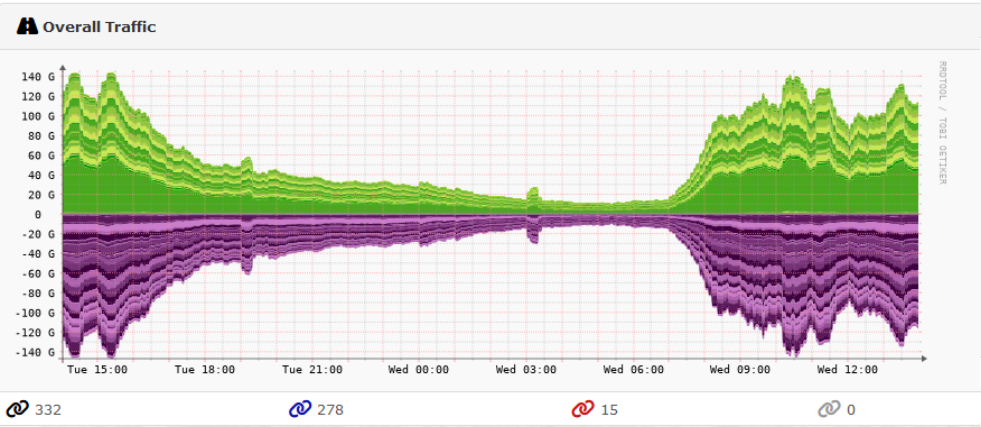
* 架設 LibreNMS 提供區網連線單位網路品質監控
* Open Source WAF
  * 從區網網站推廣至其他單位

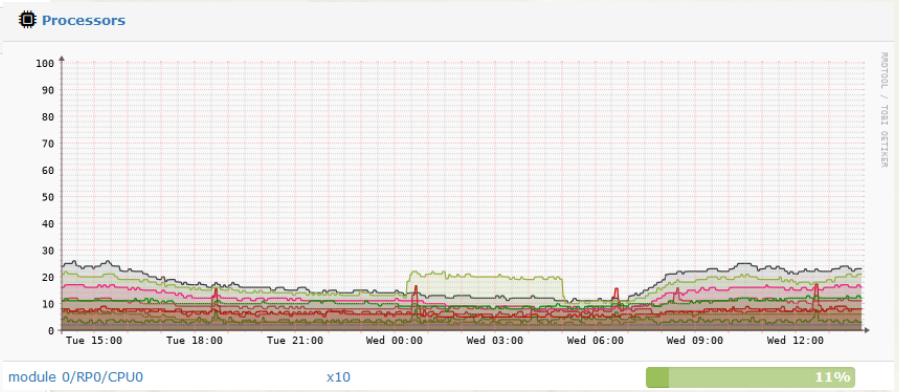
4. 特色服務
架設LibreNMS以提供區網監控

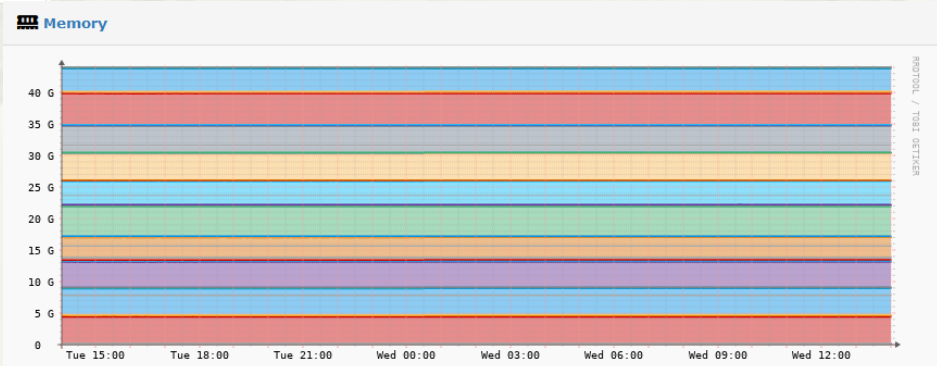
* LibreNMS透過SNMP蒐集區網ASR相關資訊
* 架設告警系統以即時偵測設備狀況與流量
* 建立即時流量圖表

現有LibreNMS功能

* SNMP蒐集區網Router資訊，以即時監測設備狀態與告警

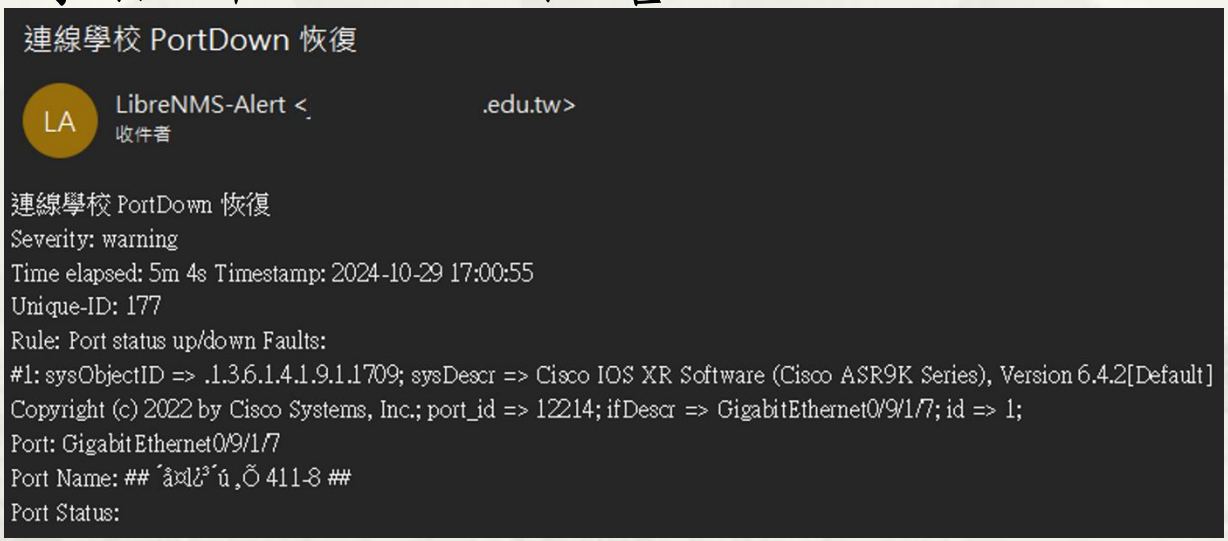


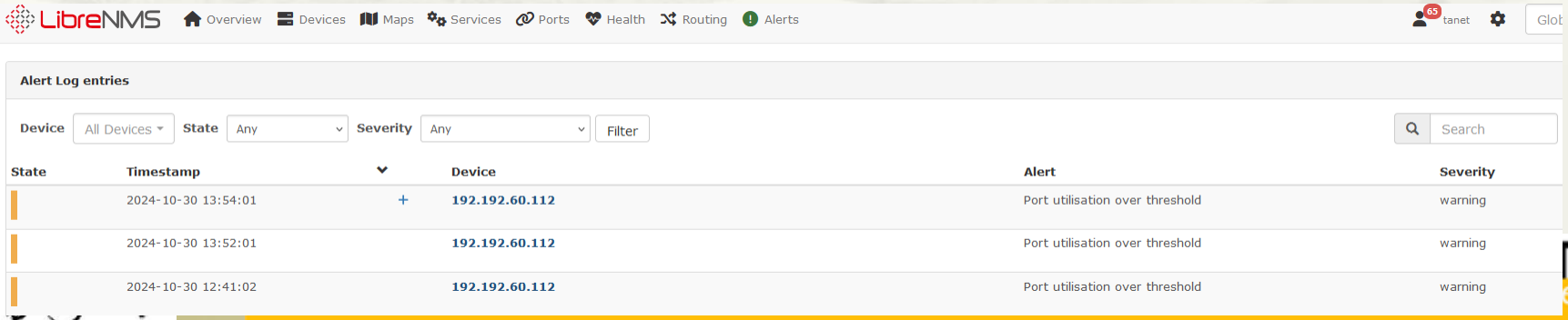




現有LibreNMS功能

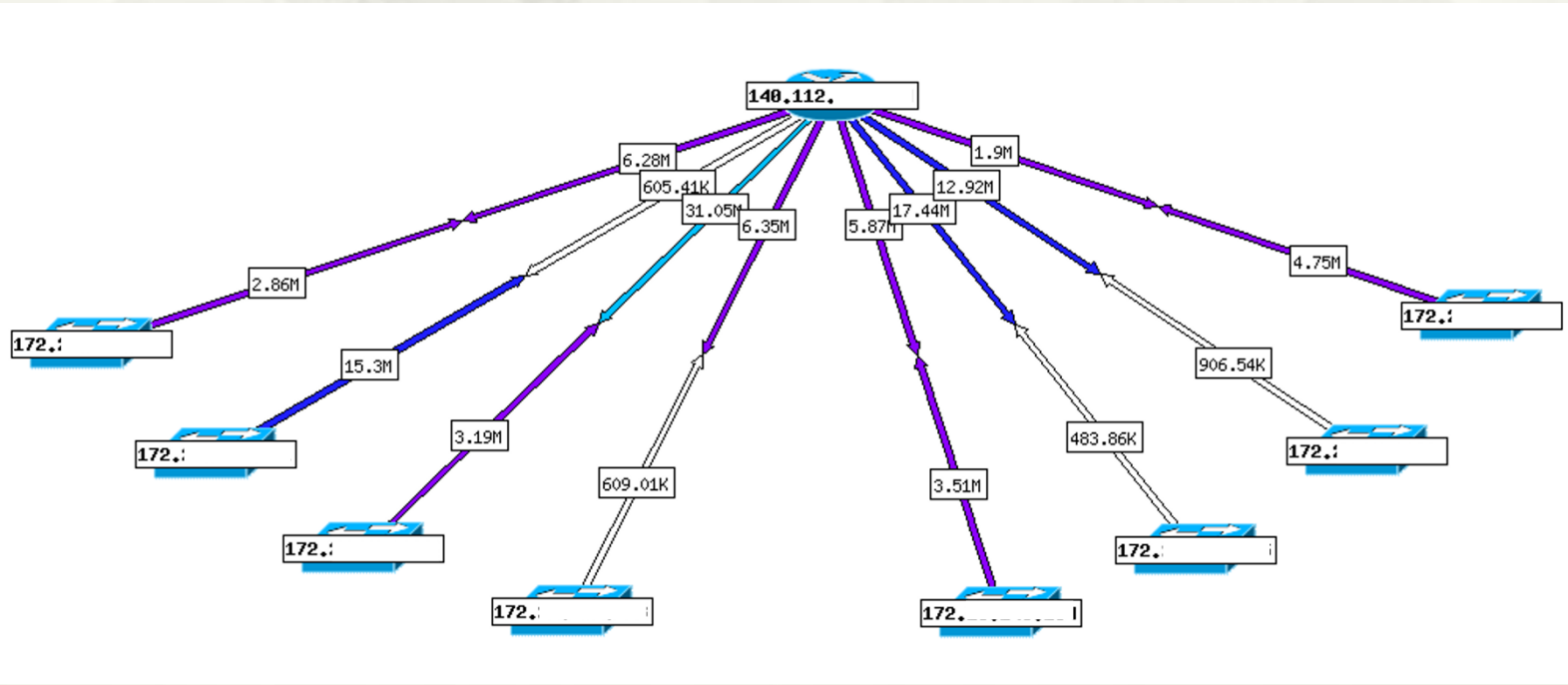
* LibreNMS自動告警機制，建立斷線、流量異常等信件、Line告警





未來待完成之LibreNMS功能

* 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。

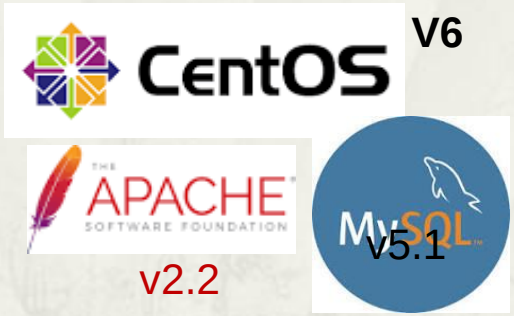


特色服務
Open Source WAF

從區網網站推廣至其他單位

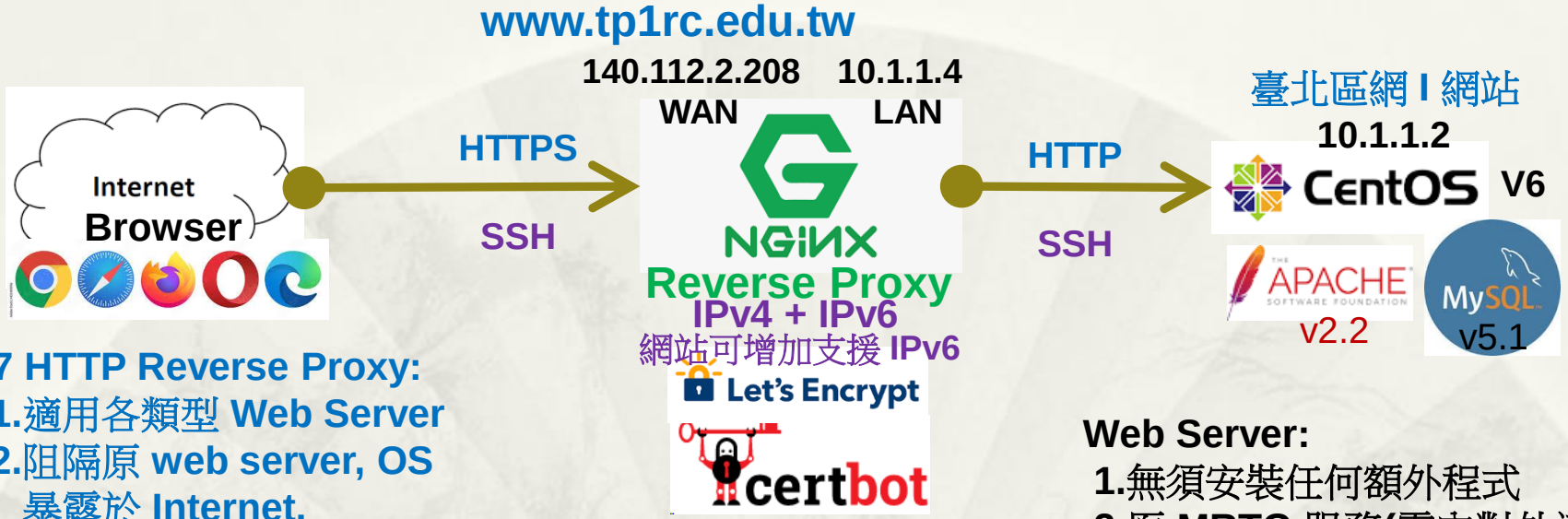
網站安全
Web Site Security

* 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)**
* 20204/07 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



* 區網網站潛在風險
  * 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

台北區網 I 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

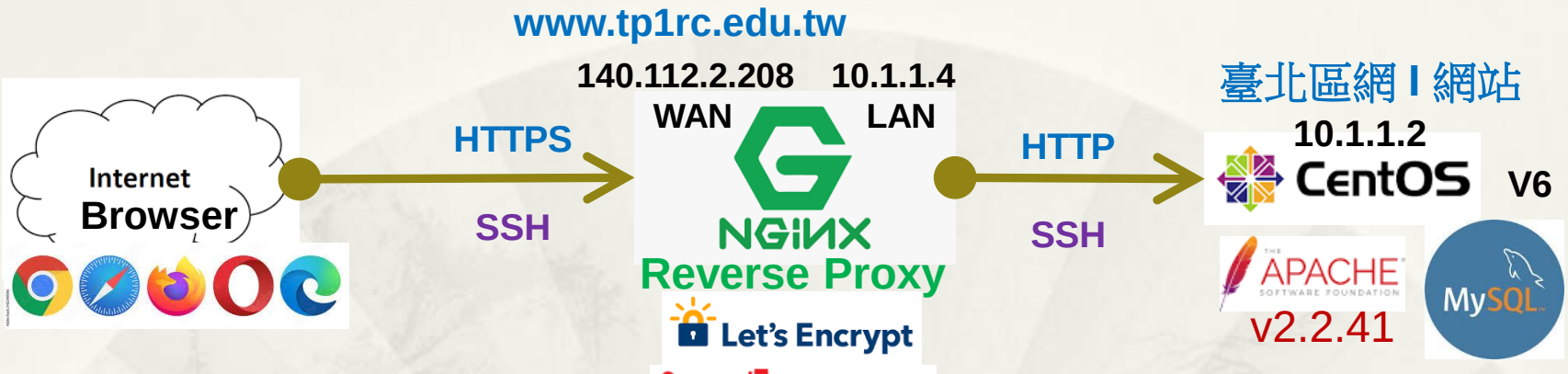
Let's Encrypt 免費憑證：

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.支援 Zero Trust 架構: 改用虛擬 IP，移除 Gateway IP 設定.
※可避免未知後門/木馬持續運作 (如:Reverse Shell)

台北區網 I 網頁新架構



ModSecurity:

1. Open Source WAF Project
2. 支援 Apache、IIS、NGINX 等網站伺服器
3. 彈性部署各類阻擋規則 Rule Set
   - (1)OWASP ModSecurity Core Rule Set
   - (2)Atomicorp's Free ModSecurity Rule
   - (3)Comodo Free ModSecurity Rules
   - (4)WordPress ModSecurity Rule Set (WPRS)

OWASP Core Rule Set(CRS)
OWASP 撰寫之阻擋規則

Docker 架構

1. 跨平台相容
2. 部署簡單快速

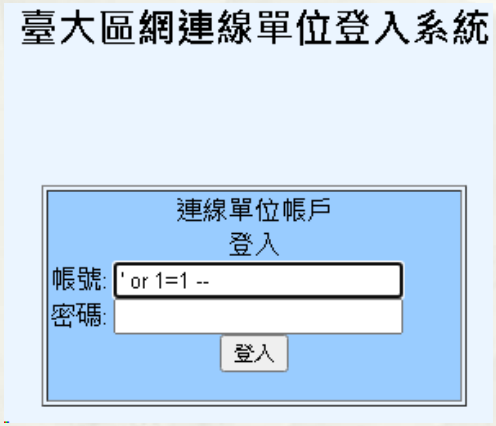
L7 HTTP Reverse Proxy
阻隔原網站 Web Server, OS 暴露於 Internet

原始網站

L7 Reverse Proxy

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

系所網站面臨問題

* 網站作業系統、Web Server、動態程式，版本老舊無法升級，需重新安裝、程式需重新改寫
* 原網站開發人員離職、無維護廠商
* 經費不足

客戶名稱 國立臺灣大學　　公司電話 [redacted]　　手機號碼

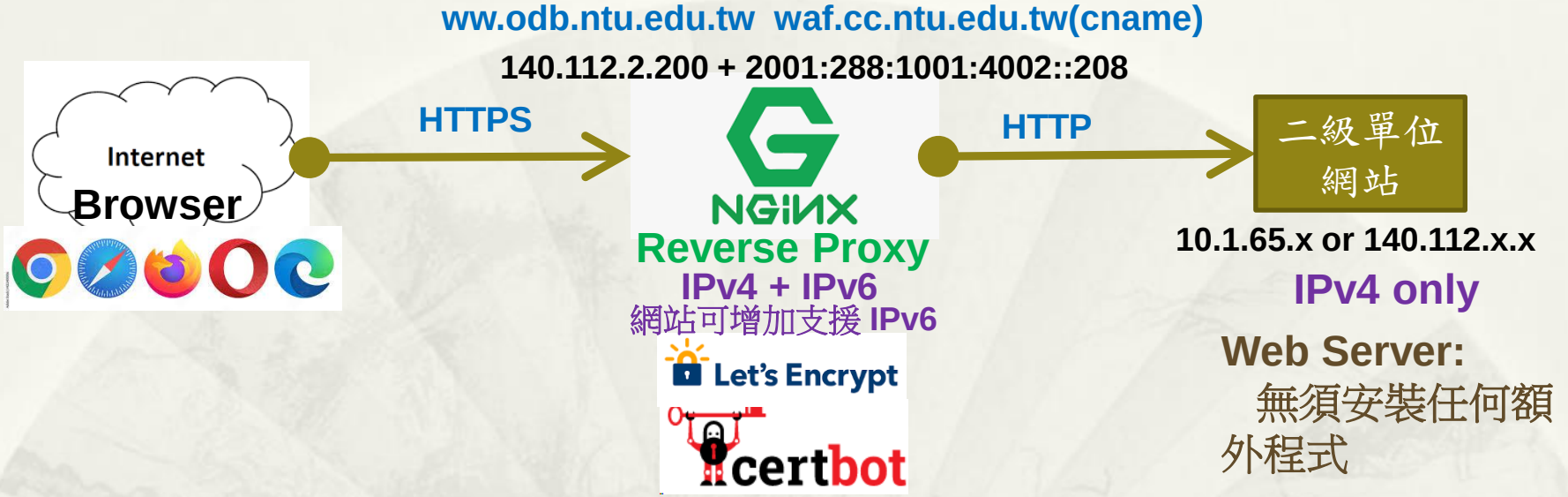
聯絡姓名 [redacted]　　電子信箱 [redacted]

製作項目	內容說明	數量	單價	金額
服務項目				
弱點掃描	1. 盲目的 SQL 注入 ：程式修補，當錯誤轉為404畫面 2. 將元件升級到最新穩定版本：以計中建議將站台js隱藏版號方式修正。 ★ 若複測後仍需要重新調整架構則另計評估 3. 系統主機增加SSL在header 以上不含中風險處理，若後續需調整則另計	1	$ 38,000	$ 38,000
			小計	$ 38,000
		含稅	5.00%	$ 1,900
			折扣 -	$ 1,900
			含稅總計	$ 38,000

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



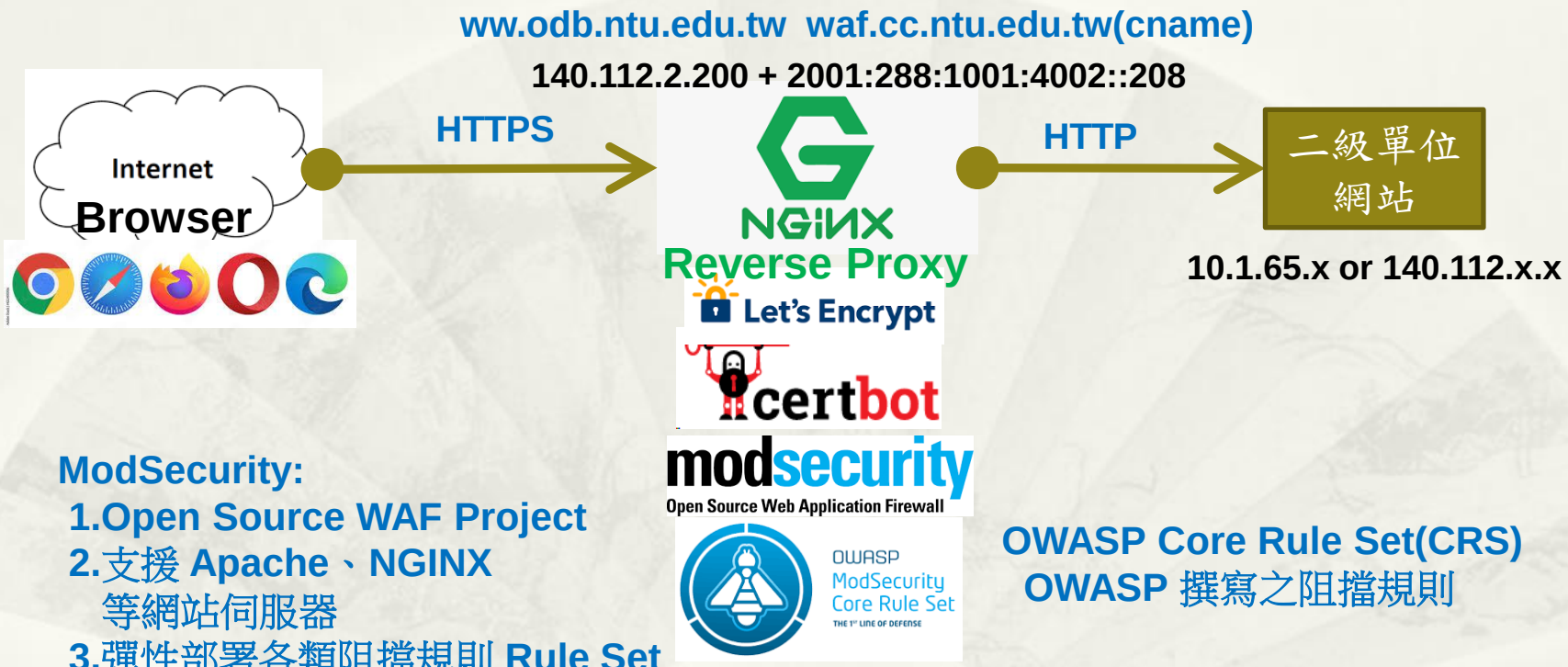
L7 HTTP Reverse Proxy:

1. 適用各類型 Web Server
2. 阻隔原網站 Web Server, OS 暴露於 Internet.
3. 額外提供 Load Balance、Content Cache、WAF 功能.

Let's Encrypt 免費憑證：

1. Certbot 安裝於NGINX，不影響原網站.
2. 憑證到期自動 Renew.
3. 減輕後端 Web Server SSL/TLS 加解密 Loading.
4. 後端已解密封包可進行 IDS/IPS 異常分析.

Open Source WAF 網頁防護架構



快速導入 WAF 防護機制

- DNS 設定
  - 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)
  - 或改成 10.1.x.x

AppScan 掃描結果比較

* 原網站

	問題類型	問題數目
重	有漏洞的元件	144
高	API 不當資產管理	2
高	發現不存在網域的鏈結	1
高	盲目的 LDAP 注入	3
中	CORS 原則是依據任意原始標頭所設定	1
中	Microsoft Windows MHTML 跨網站 Scripting	1
中	SameSite 屬性不安全、不適當或遺漏的 Cookie	1
中	不安全的第三方鏈結 (target="_blank")	47
中	偵測到 SHA-1 密碼組合	1
中	啟用 TRACE 與 TRACK HTTP 方法	1
中	找到目錄清單型樣	2
中	機密性標頭上的 ADNS 盲目 SSRF	12
中	檢查是否有 SRI（子資源完整性）支援	15
中	目錄清單	2

200+ 中高風險

* 導入 WAF 後

	問題類型	問題數目
重	有漏洞的元件	80
中	偵測到 SHA-1 密碼組合	1
中	檢查是否有 SRI（子資源完整性）支援	7

80+ 中高風險

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
```

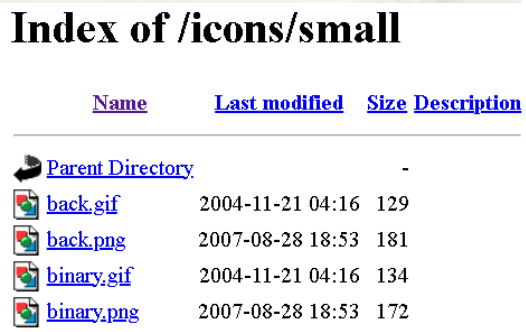
Response

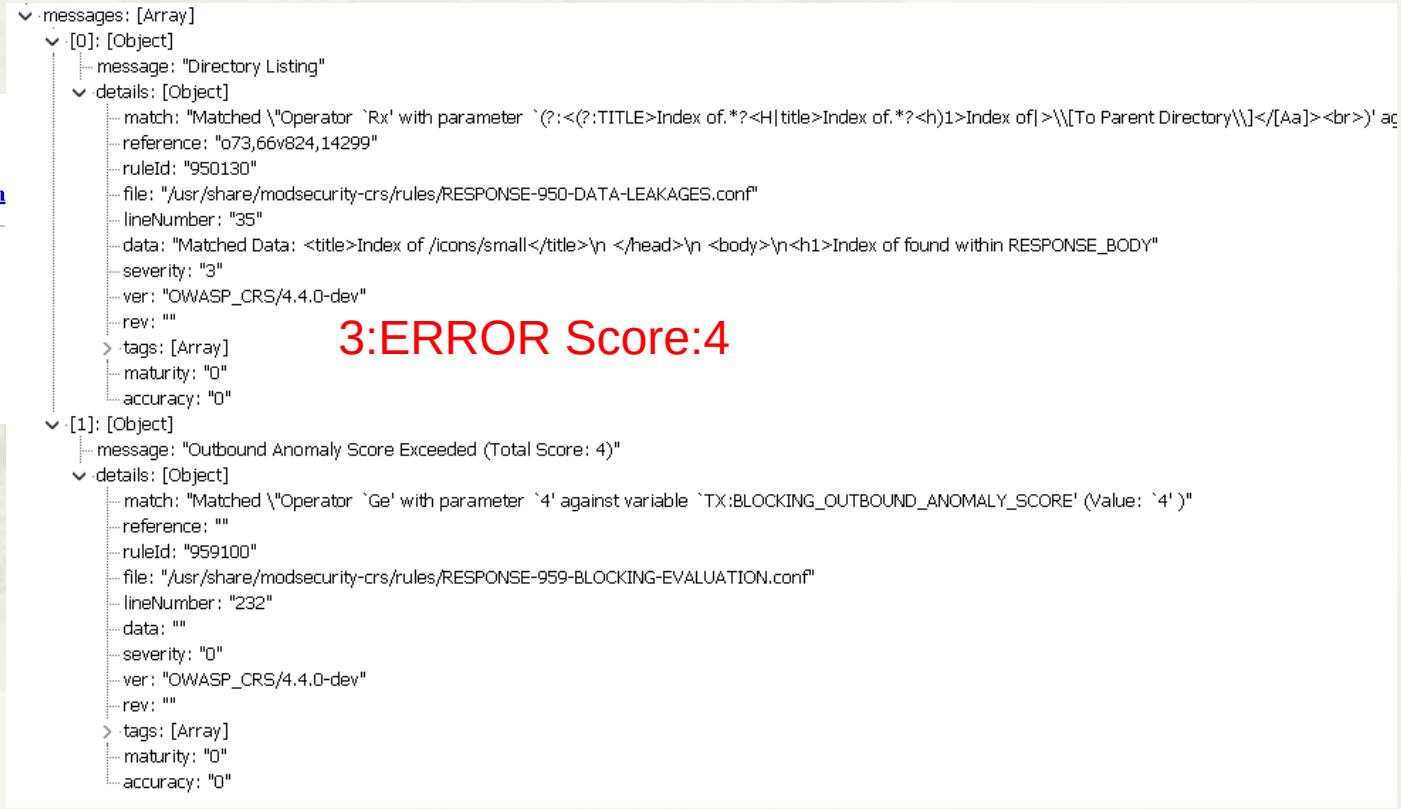
Pretty Raw Hex Render

```
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/





5.成效精進

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。	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 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。

112年評審委員建議與回覆

No	委員建議	回覆
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。

112年評審委員建議與回覆

No	委員建議	回覆
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。	謝謝委員建議，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。

112年評審委員建議與回覆

No	委員建議	回覆
		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。	謝謝委員建議，已經修改完成。 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。

112年評審委員建議與回覆

No	委員建議	回覆
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。

112年評審委員建議與回覆

No	委員建議	回覆
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 評估何者較接近連線學校網路使用者實務連網的網速。	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 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。

112年評審委員建議與回覆

No	委員建議	回覆
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。

6.基礎維運
大綱

* 區網服務VM主機群由 Vmware ESXi 移轉至 Proxmox Virtual Environment(PVE)
  * 網頁主機、WAF 防護、MRTG、Cacti
* 2024/09/24 中華電信斷線四小時，影響 11 間連線單位
* 2024/02/18 ASR 韌體升級過程與障礙排除
* 113 營運目標達成報告

VMware 之近況

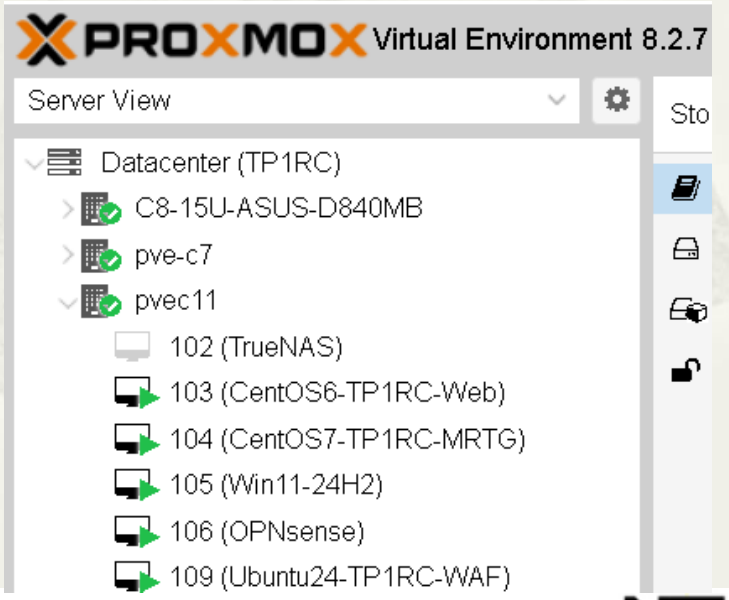
- 2022 博通Broadcom宣佈以 610億美元(溢價50%）併購 Vmware (Broadcom 市值 2200億)
  - 博通已分別收購軟體公司 CA Technologies，賽門鐵克企業端安全業務
- 2023/11 收購完成後一周裁減VMware人力，據稱超過2,000人。未經證實的消息指出博通以不續工作簽證為手段，迫使外籍工程師主動離職。
  - https://www.reddit.com/r/vmware/comments/1b1sah4/broadcom_silent_layoffs_email_to_vmware_about_40/?rdt=61195
- 2023/12 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)

- Linux Debian + QEMU/KVM + LXC(Linux Container)
- Open Source vs. 商業版本: 功能完全相同
- 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

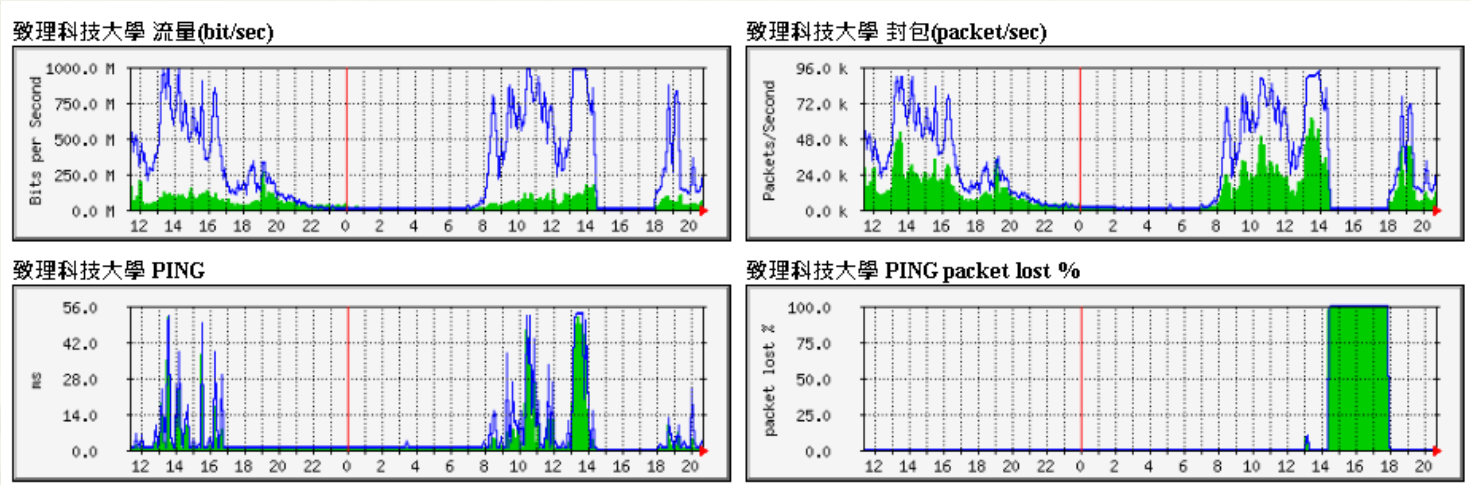


Proxmox VE

不需額外付費，內建即支援之功能

* 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

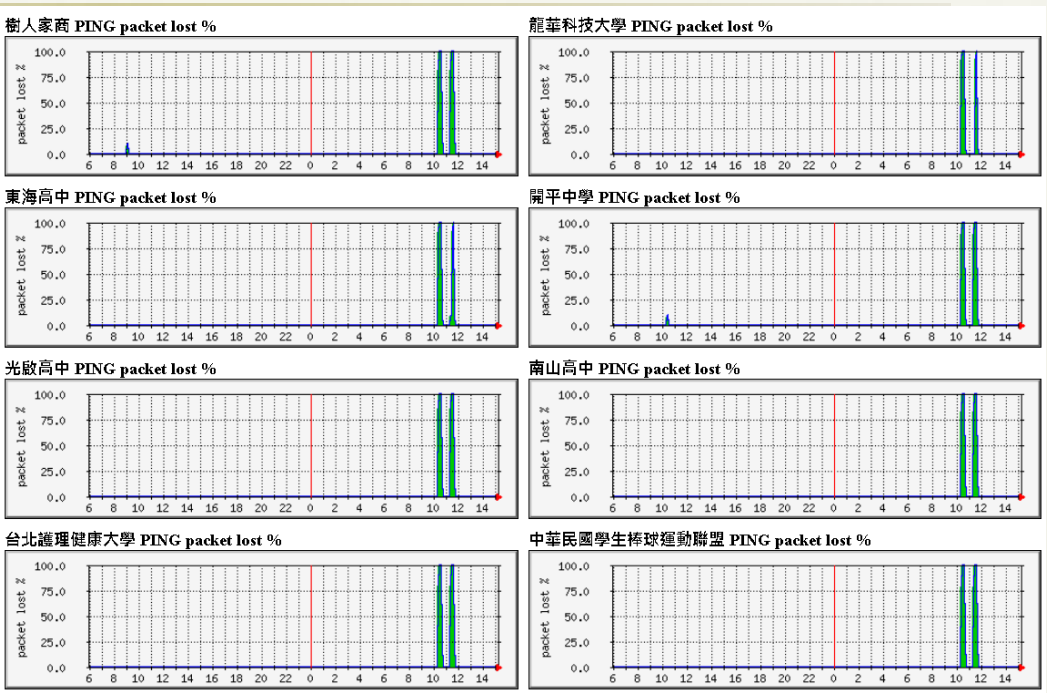
2024/09/24
中華電信斷線持續四小時以上



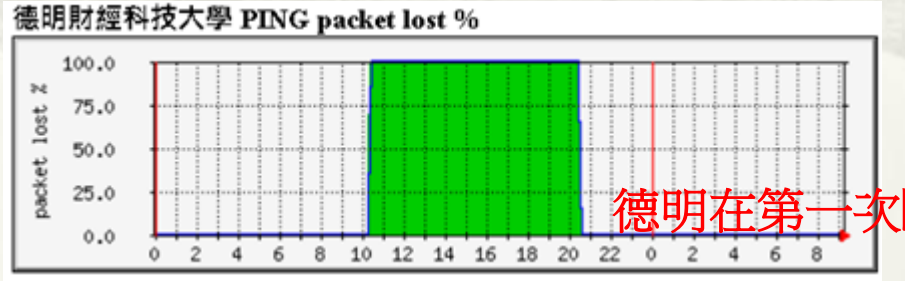
* 共有11 間學校受到影響
  * 致理科技大學、龍華科技大學、台北護理健康大學
  * 臺灣藝術大學、德明財經科技大學、國立空中大學
  * 國防大學管理學院、東吳大學(城中校區)
  * 宏國德霖科技大學、康寧大學-台北校區、臺灣大學醫學院校區
* 中華電信檢討報告回覆，因設備設定異常造成

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)

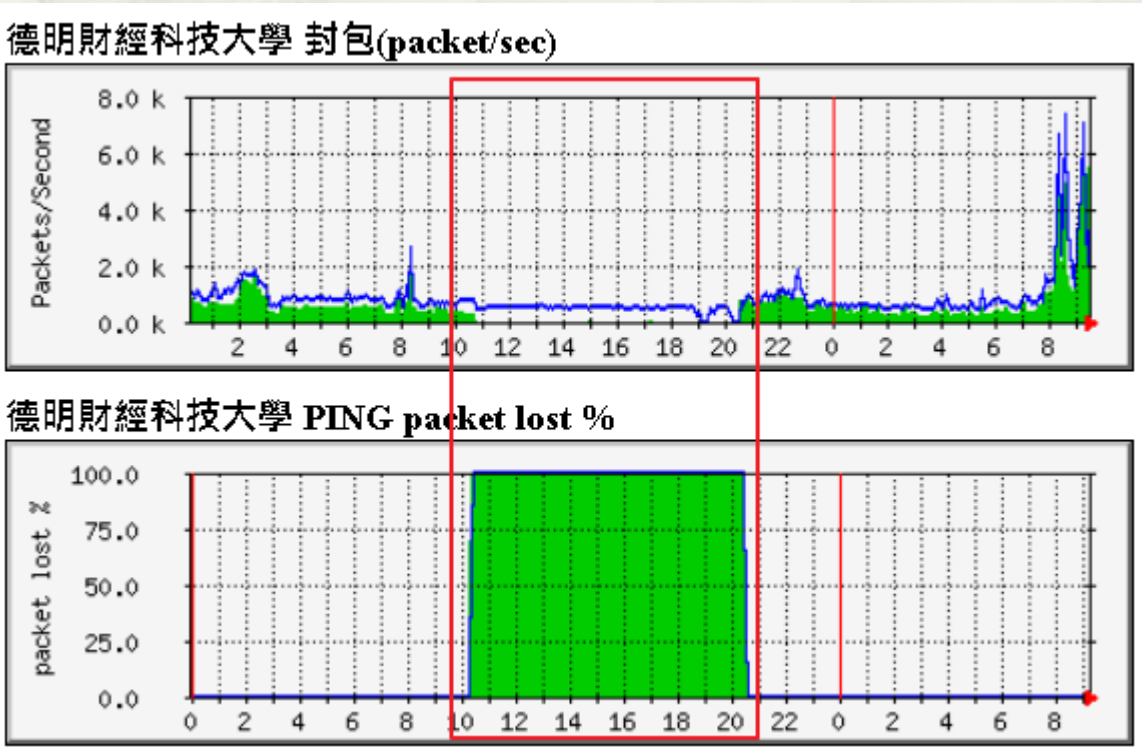


* 德明科大



德明科大 MRTG
封包流量與封包遺失

* 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

* 台大電信機房之中華電信設備 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

113 營運目標 達成報告

* 網路妥適率: 99.99%以上
  * 達成，骨幹線路與設備皆正常 100%
* 區網網管會議出席率: 90%以上
  * 達成，出席率 94.5%
* 大專院校 ipv6 使用率: 100%
  * 未達成，僅剩一間學校(軍事情報局)
* 高國中小 ipv6 使用率: 80%以上
  * 達成，使用率 90%
* 區網網路與資安課程: 10場以上
  * 達成， 共開設 17門課程

評審委員: 對本年度區網維運相關工作任務成果，能有檢討與建議

113 營運目標 達成報告

* 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
* 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。
* 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。
* 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。

評審委員: 對本年度區網維運相關工作任務成果，能有檢討與建議

7.對連線學校服務的支持

* 113年度區網暑期課程
* 區網網管會議
* 滿意度調查
* “高中體育總會”離開 TANet 事件

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 打造超流暢工作流 (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 技術總監 鄭郁霖	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 (線上實做)	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 Gmail 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	鋐迪資訊 資深技術顧問 鍾迪	80

113年度區網課程(17門)

分類	講題	講者	出席
雲端	無痛連結 Google Workspace, REST APIs（初階）(線上實做)	CloudMile 陳智聰	71
雲端	無痛連結 Google Workspace, REST APIs（進階）(線上實做)	CloudMile 陳智聰	55
系統	以Pure Storage 平台來加速擁抱 AI 的驅動力	Pure Storage 蔣燄峰	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、常用工具與原理介紹	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

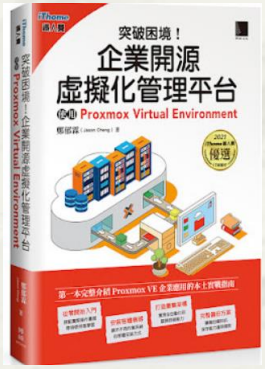
每堂課平均 66人

113年度區網課程(17門)總結

* 豐富多元之資訊相關應用課程

類別	雲端	資安	大數據	系統	法規	網路
堂數	6	6	1	2	1	1

* 線上、Lab實作多達10堂
* 掌握資訊熱門趨勢、最夯技術
  * Google 雲端應用技術
  * Gemini(生成式AI) 應用實例
  * Proxmox VE 入門實作課程 (LAB實做)
    * 節省工具箱公司 技術總監 鄭郁霖(節省哥)
  * 網頁架站工具 WordPress 漏洞修補技巧
    * 計中同仁技術交流課程



區網網管會議

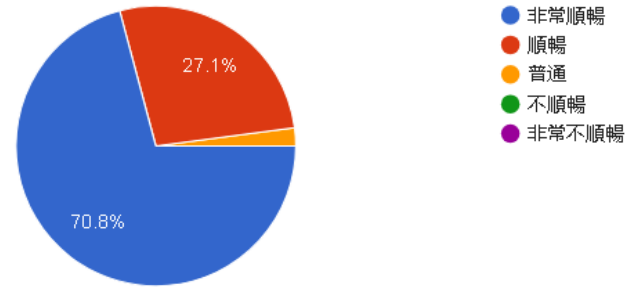
* 113年第一次網管會議出席率: 94.5%
  * 實體與線上會議同步進行
* 安排連線單位輪流技術交流分享
* 過去曾經分享過的單位與主題
  * 臺北醫學大學 --北醫大雙校區機房整建與資安健檢經驗分享
  * 台大醫院 -- 從 syslog 到網路聯防機制
  * 大考中心 -- 教育部資通安全稽核技術與經驗分享
  * 台師大 -- 大考中心 - 教育部資通安全稽核技術與經驗分享
  * 臺北海洋科技大學 – 校園網路骨幹建置與宿舍網路建議經驗分享

連線單位滿意度調查結果 part1

* 54連線單位，收到 48 份回覆 (回覆率 89%)

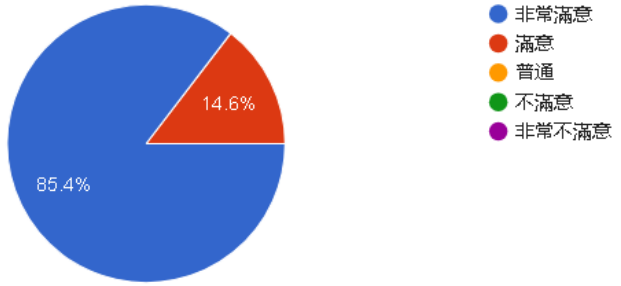
本年度　貴單位之網路連線服務，順暢與否?

48 則回應



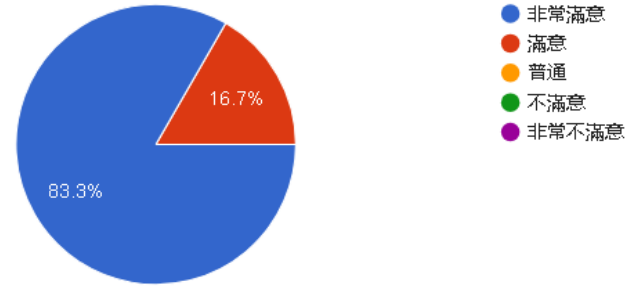
資通安全事件的通報應變的協助處理:

48 則回應



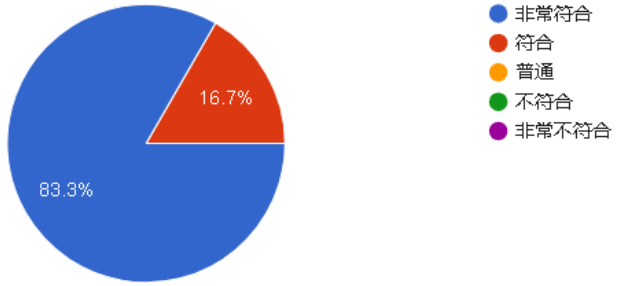
本年度　貴單位如有網路管理或連線問題時，區網中心的協助是否有順利排除障礙?

48 則回應



對區網所舉辦之教育訓練或研習課程，是否能符合　貴單位實務運作上的需求?

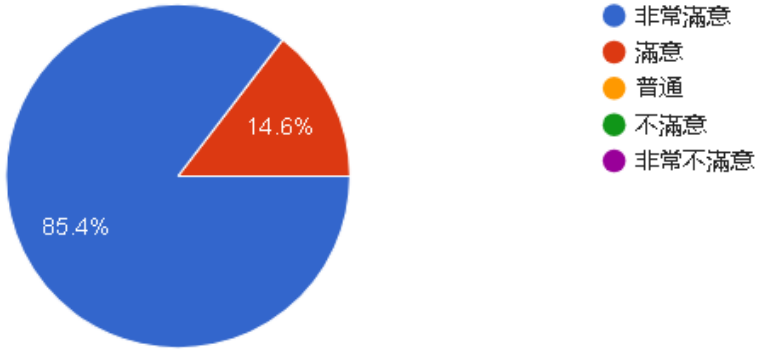
48 則回應



滿意度調查結果 part2

貴單位對於區網中心服務人員之熱忱及親和力的滿意度?

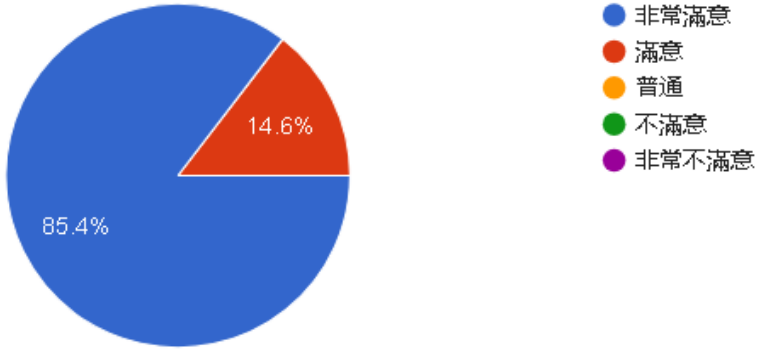
48 則回應



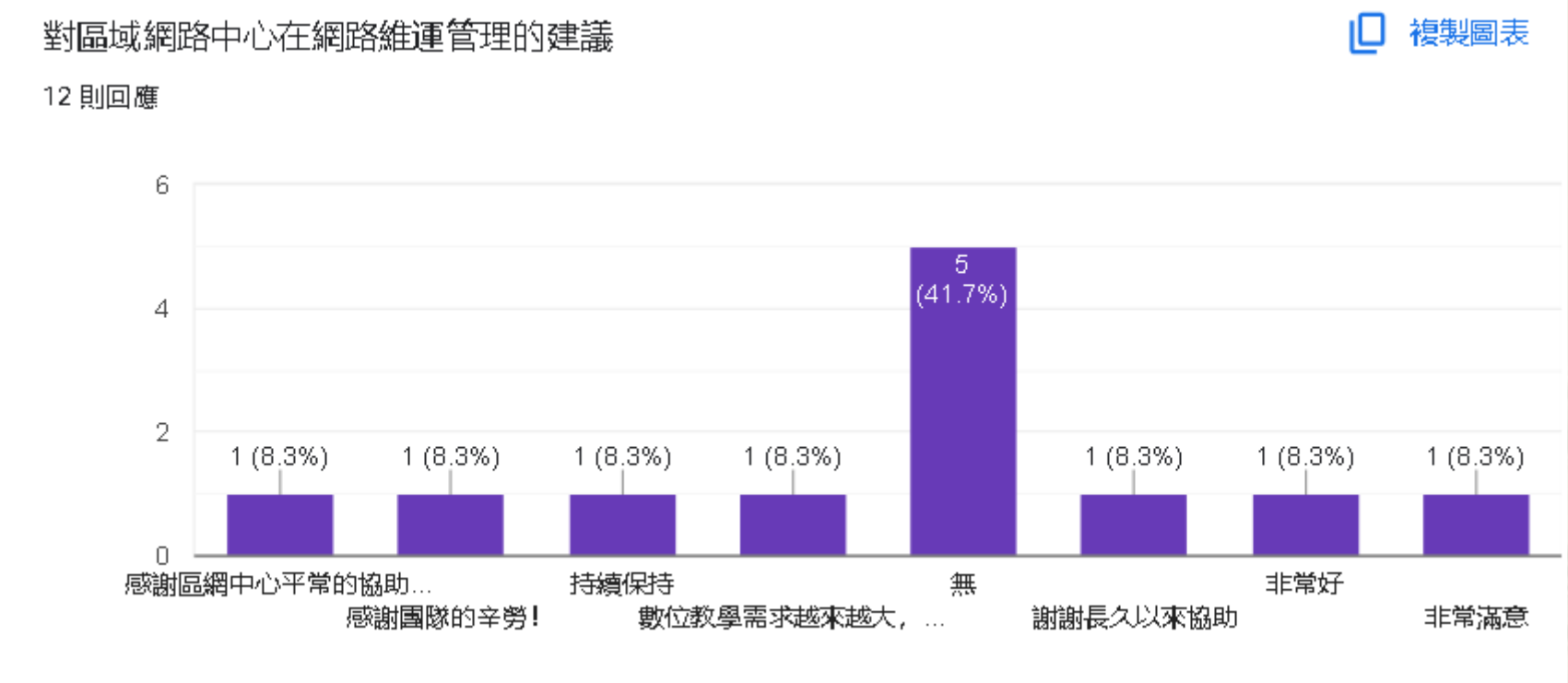
貴單位對於區網中心綜合整體服務的表現

48 則回應

整體服務 非常滿意 85.4%



滿意度調查結果 part3



“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學網網段(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

* 提供很多 Pubic IP
  * 但也許現況不需太多 IP (雲端網站、NAT 技術)
* 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

- 需遵循教育部連線單位使用規範、資安法及資安稽核
- 非無償免費接上 TANet，電路費較租用 ISP 服務貴上 10 倍
  - 光世代 300M: 每月 $999
  - Peer 電路 300M: 每月 $10,000
- 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1: TANet Telstra 電路
國際頻寬壅塞

* 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

補充2: 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

8.1 未來營運目標

- 網路妥適率: 99.99%以上
- 區網網管會議出席率: 90%以上
- 大專院校 ipv6 使用率: 100%
- 高國中小 ipv6 使用率: 80%以上
- 區網網路與資安課程: 10場以上
- 區網課程 Lab 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
- 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

8.2 其他建議

* 各節點 Peer IP 應加上 IP 反解名稱，才能知道經過路徑.

```
C:\Users\Administrator>tracert line.me

在上限 30 個躍點上
追蹤 line.me [203.104.138.138] 的路由:

  1    <1 ms    <1 ms    <1 ms  192.168.20.1
  2     1 ms    <1 ms    <1 ms  nep17-254.tp1rc.edu.tw [163.28.17.254]
  3     2 ms     1 ms     1 ms  192.192.61.82
  4     3 ms     3 ms     3 ms  192.192.61.185
  5     1 ms     1 ms     1 ms  192.192.61.194
  6    53 ms    53 ms    52 ms  202.169.174.154
  7     *        *        *     要求等候逾時。
  8     *        *        *     要求等候逾時。
  9  ^C
```

僅顯示 IP
無法知道經過路徑

簡報完畢
謝謝