112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、李墨軒

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.對連線學校服務的支持度
* 8.未來營運計畫與建議

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
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	1,240,866	529,918	69%	99%
112	1,792,000	1,131,871 (10月底)	49,307	95%	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，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%

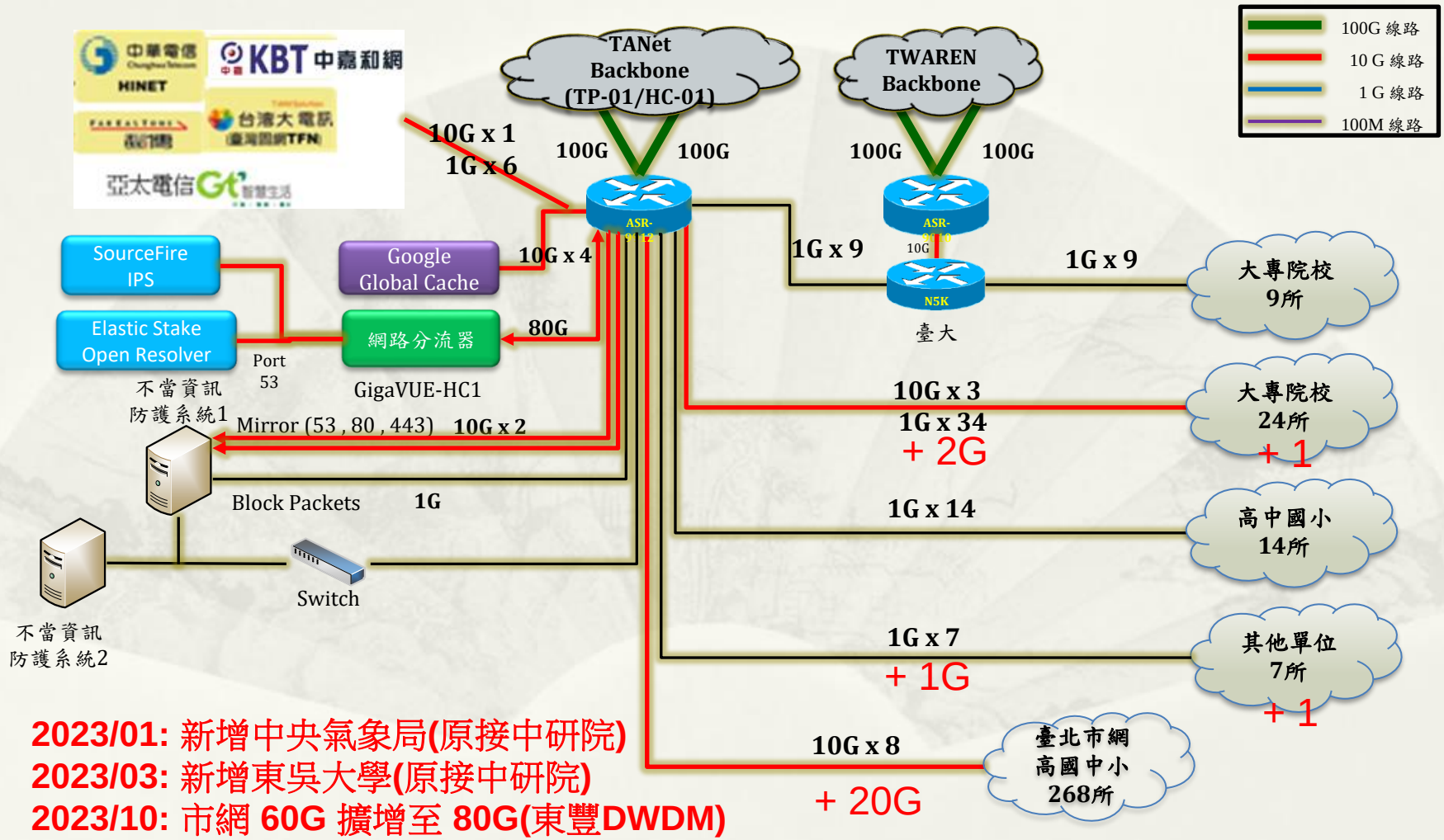
1.2 區網人力

* 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：李墨軒
  * E-mail：molee@ntu.edu.tw
  * 電話：(02) 33665012
* 編制內專職及約聘僱人員8名

2.網路管理

* 1.網路架構
* 2.網路流量
* 3.IPv6 完成率
* 4.Google Global Cache 2022 建置完成

台北區網 I 網路架構



2023/01: 新增中央氣象局(原接中研院)
2023/03: 新增東吳大學(原接中研院)
2023/10: 市網 60G 擴增至 80G(東豐DWDM)

如何節省電路租賃成本

- 台北市網電路租賃現況: 10G x 8
- 可考慮使用 Single Dark Fiber
- DWDM Single Fiber
  - 8 Channels: Use 16 Waves

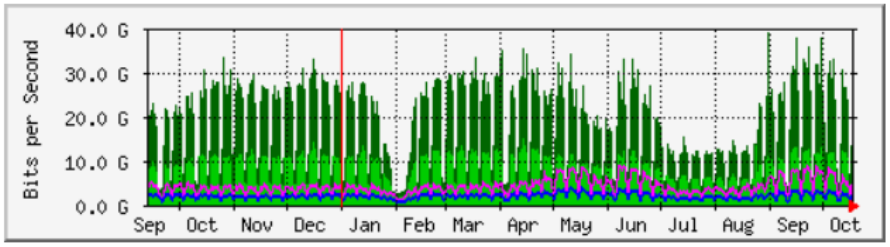
節省光纖 Dark Fiber 蕊數

* 單蕊光纖 Transceiver: SFP 成套(一對)

2023 網路流量比較

IPv4 流量

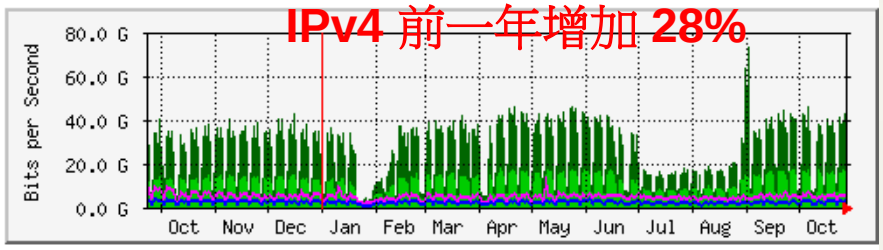
`Yearly' Graph (1 Day Average) 2022



	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

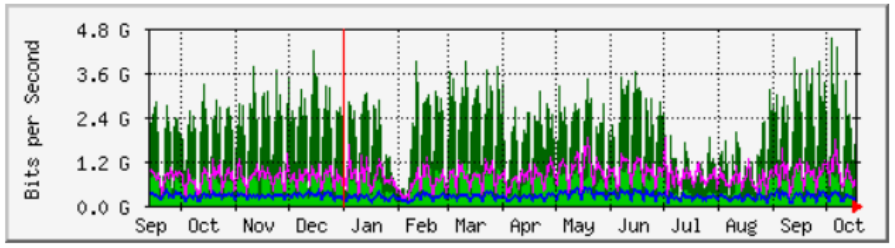
IPv4 前一年增加 28%



	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

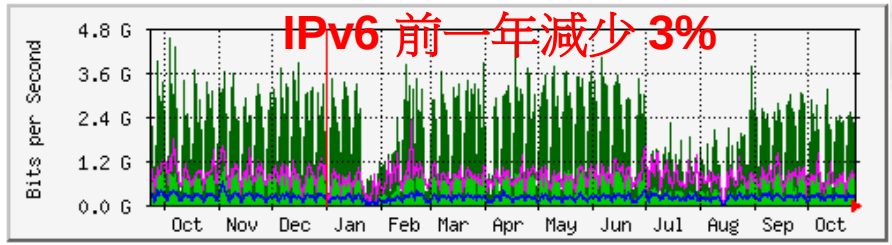
`Yearly' Graph (1 Day Average) 2022



	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%

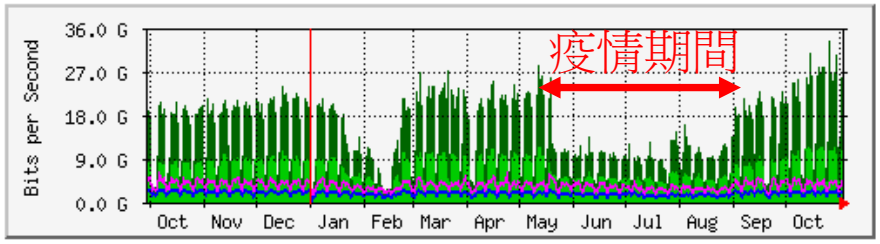


	Max	Average	Current
台北主節點 => 北區區網	4541.2 Mb/s (4.5%)	516.2 Mb/s (0.5%)	681.2 Mb/s (0.7%)
北區區網 => 台北主節點	2242.3 Mb/s (2.2%)	182.9 Mb/s (0.2%)	224.6 Mb/s (0.2%)

2022 網路流量比較

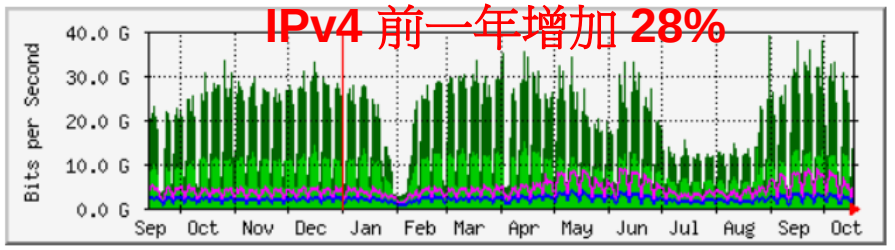
IPv4 流量

`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%)

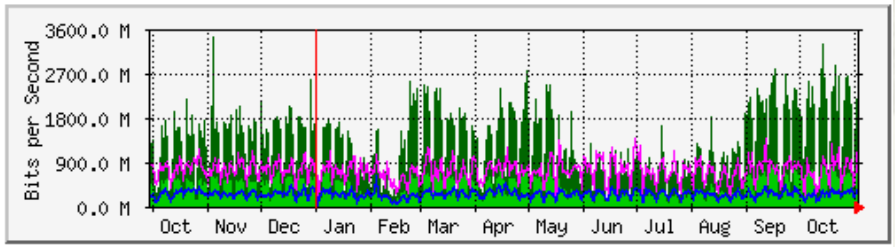
`Yearly' Graph (1 Day Average) 2022



	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%)

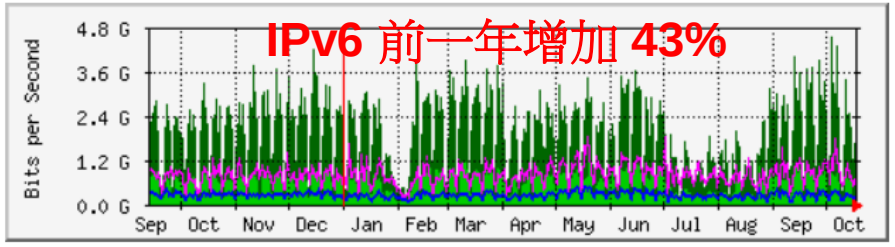
IPv6 流量

`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

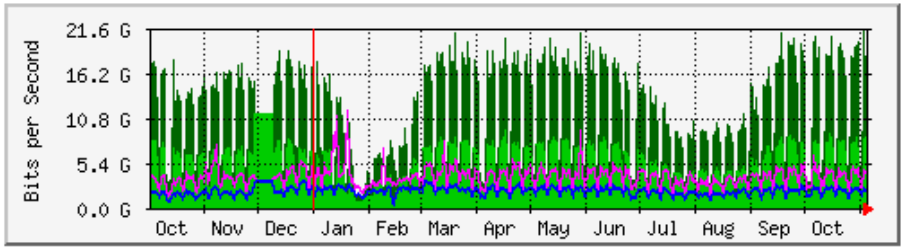


	Max	Average	Current
台北主節點 => 北區區網	4541.2 Mb/s (4.5%)	533.3 Mb/s (0.5%)	785.2 Mb/s (0.8%)
北區區網 => 台北主節點	1804.7 Mb/s (1.8%)	233.6 Mb/s (0.2%)	243.3 Mb/s (0.2%)

2021 網路流量比較

IPv4 流量

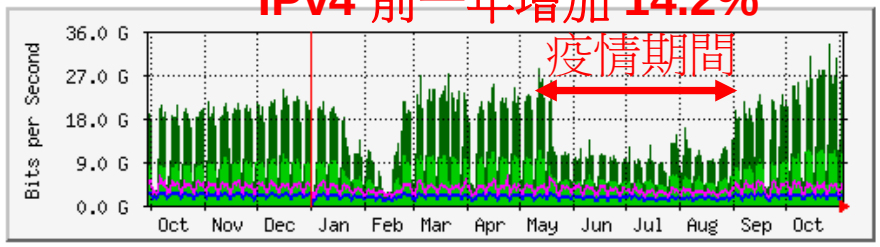
每年 圖表 (1 天 平均) 2020



	最大	平均	目前
台北主節點 => 北區區網	21.3 Gb/秒 (21.3%)	5352.9 Mb/秒 (5.4%)	8451.7 Mb/秒 (8.5%)
北區區網 => 台北主節點	11.5 Gb/秒 (11.5%)	1958.4 Mb/秒 (2.0%)	2076.6 Mb/秒 (2.1%)

`Yearly' Graph (1 Day Average) 2021

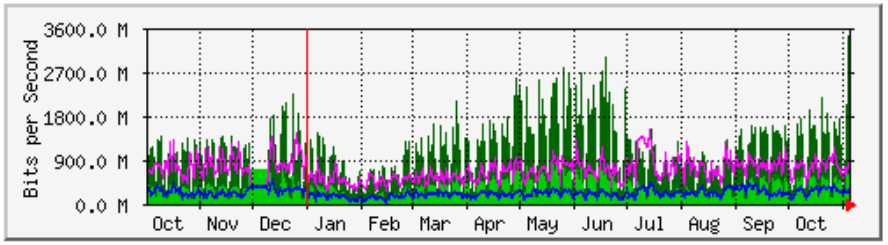
IPv4 前一年增加 14.2%



	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%)

IPv6 流量

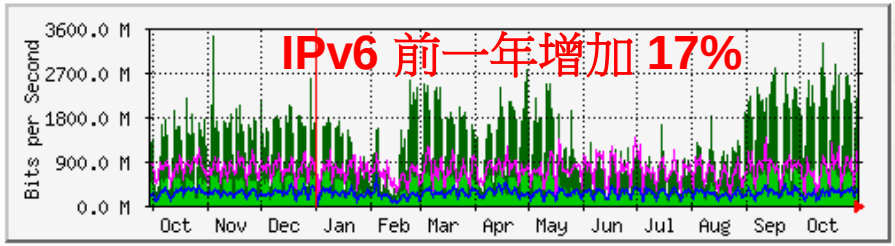
每年 圖表 (1 天 平均) 2020



	最大	平均	目前
台北主節點 => 北區區網	3431.8 Mb/秒 (3.4%)	320.0 Mb/秒 (0.3%)	566.0 Mb/秒 (0.6%)
北區區網 => 台北主節點	1476.4 Mb/秒 (1.5%)	204.3 Mb/秒 (0.2%)	301.4 Mb/秒 (0.3%)

`Yearly' Graph (1 Day Average) 2021

IPv6 前一年增加 17%

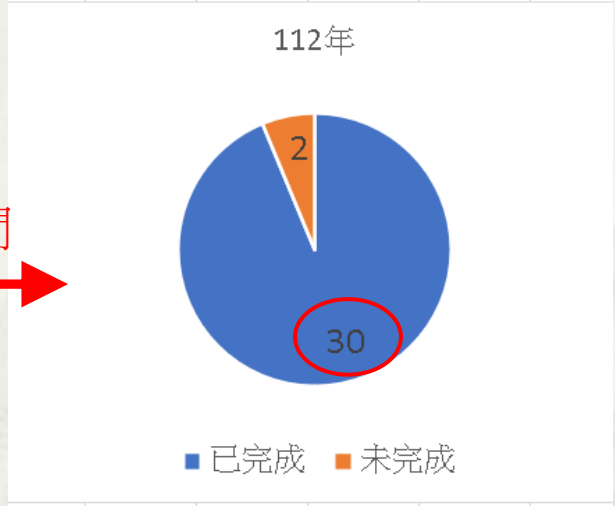


	Max	Average	Current
台北主節點 => 北區區網	3431.8 Mb/s (3.4%)	372.0 Mb/s (0.4%)	732.0 Mb/s (0.7%)
北區區網 => 台北主節點	1361.6 Mb/s (1.4%)	232.1 Mb/s (0.2%)	270.7 Mb/s (0.3%)

2.3 IPv6 大專院校完成率

* 路由網段設定完成率
  * 大專院校:32 間

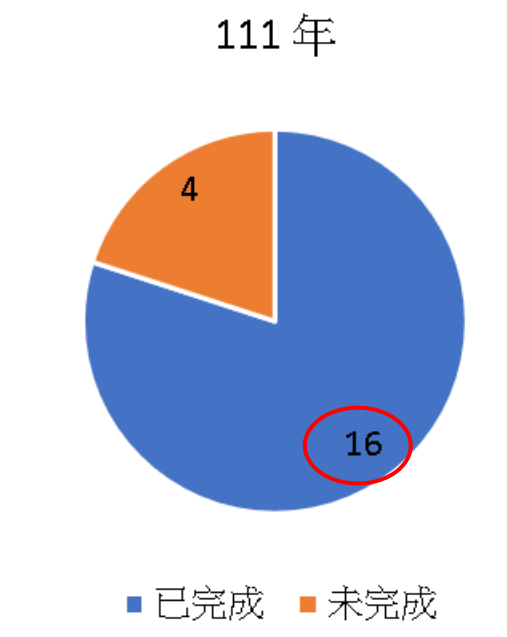
增加一間



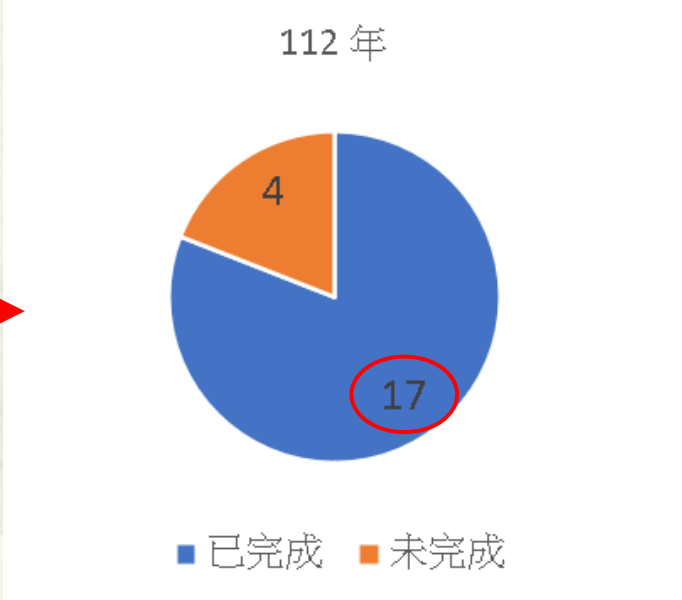
有 ipv6 網段學校全部完成
尚無 ipv6 網段:軍事情報局學校、臺北基督學院

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: 21間



增加一間



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

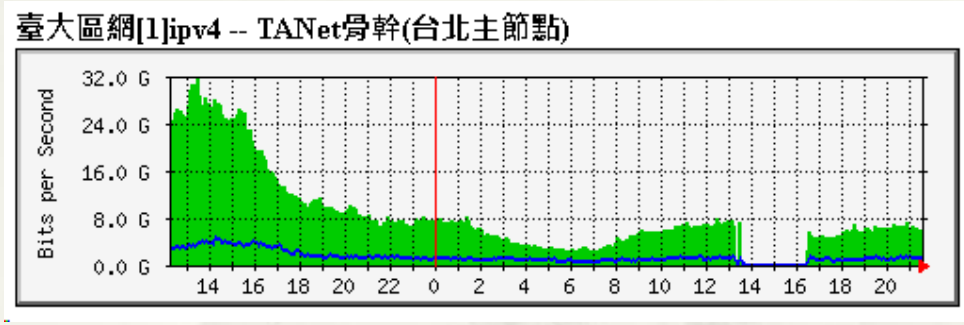
學網骨幹大斷線
台北/新竹 100G 雙斷
(5/1 勞動節三天連假)

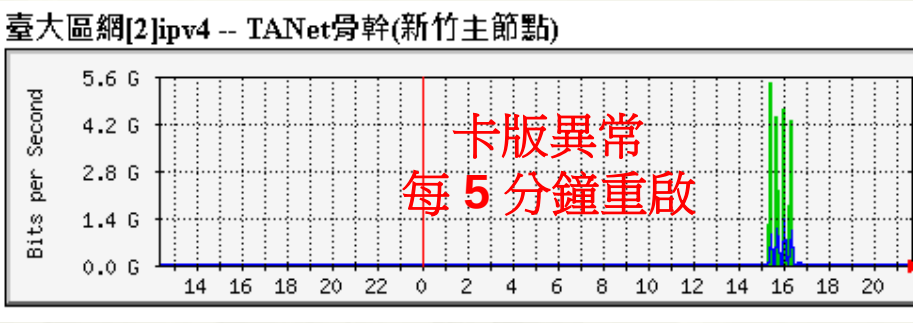
2023/04/29(六) 13:30 ~ 16:35 (3小時5分鐘)
2023/04/30(日) 10:35 ~ 10:45(10分鐘)
2023/05/01(一) 11:41 ~ 13:32(1小時51分鐘)

2023/04/29 13:30 ~ 16:35 (3小時5分鐘) TANet 骨幹斷線過程

- 2023/04/10
  - 因區網 100G 備援線路新竹主節點卡版異常, 因此 4/10 之後區網無備援線路機制.
    - [公告]新竹主節點ASR-9912-01 sloto A9K-8X100G-TR卡板運作異常
    - https://noc.tanet.edu.tw/index.php/operation-announcement/op-a/op-a-01/1555-asr-9912-01-sloto-a9k-8x100g-tr
- 2023/04/29 13:30
  - 區網與臺北主節點不明原因中斷連線.
- 2023/04/29 15:10
  - 因臺北主節點線路中斷尚在釐清問題，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，
  - 每隔 5~10 分鐘會自動重啟，導致線路斷斷續續。
- 2023/04/29 16:35
  - 臺北主節點 A4光纖線路因三峽介壽路一段邊溝施工中斷，導致斷線，目前已經恢復。
- 2023/04/29 16:45
  - 確認區網流量恢復正常

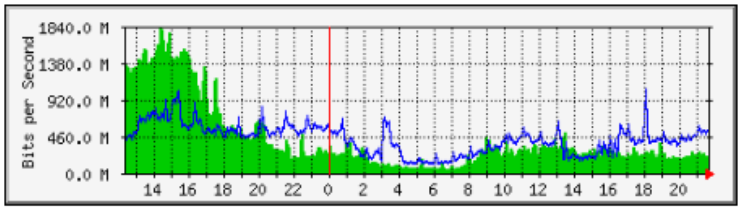
2023/04/29
台北/新竹 雙主節點 同時異常



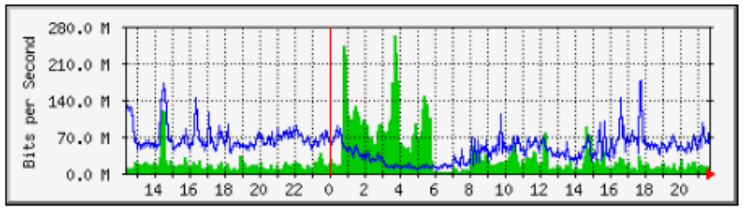


2023/04/29
ISP 連線正常

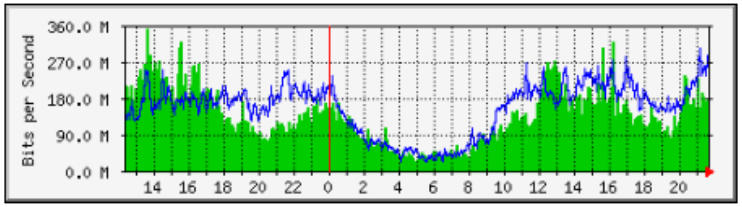
中華電信10G



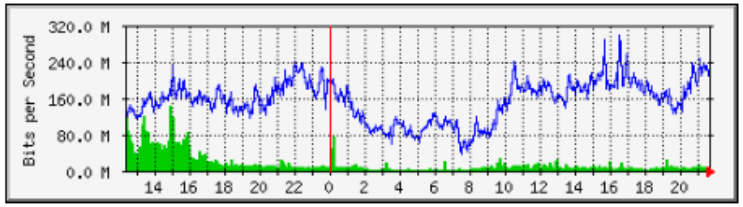
亞太電信



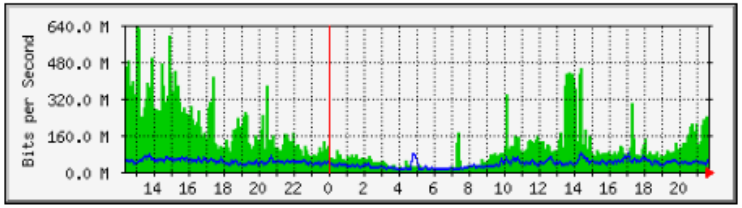
台灣固網1



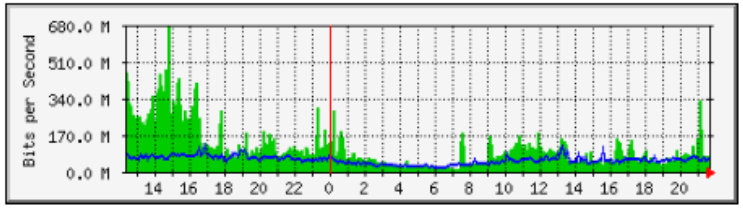
台灣固網2



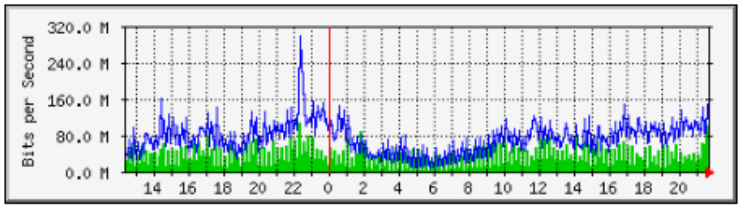
遠傳電信1



遠傳電信2



中嘉和網電信 kbtelecom



2023/04/30 10:35 ~ 10:45 (10分鐘) TANet 骨幹斷線過程

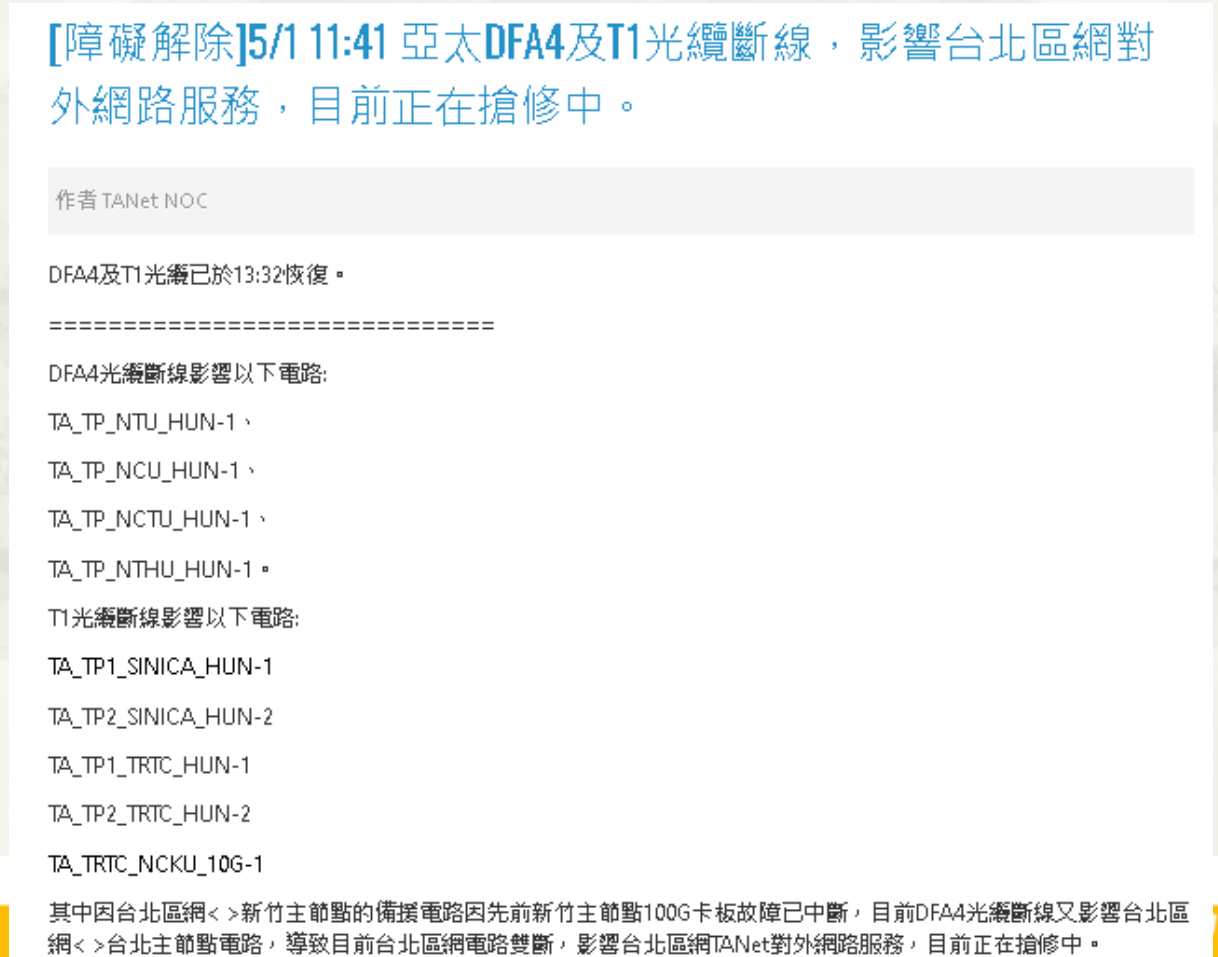
* 2023/04/30 10:35
  * 區網與臺北主節點不明原因中斷連線，新竹主節點100G 卡版因異常並未排除，無法發揮備援作用，導致對外完全中斷

2023/05/01 11:41 ~ 13:32(1小時51分鐘) TANet 骨幹斷線過程

* 2023/05/01 11:41
  * 區網與臺北主節點不明原因中斷連線，新竹主節點100G卡版雖暫時啟用，但因卡版異常並未解決，
  * 每5~10分鐘會自動重啟，導致對外連線斷斷續續。
* 2023/05/01 13:32
  * 臺北主節點恢復連線，參考TANet NOC公告，異常原因為亞太DFA4及T1光纜斷線。
    * 請參考TANet NOC公告 https://noc.tanet.edu.tw/index.php/operation-announcement/op-a/op-a-01/1557-5-1-11-41-dfa4-t1
* 2023/05/01 14:10
  * 新竹主節點100G卡版更換完成，備援線路啟用，若再發生臺北主節點斷線，應可自動切換至新竹主節點。

2023/05/01
TANet NOC 公告

* https://noc.tanet.edu.tw/index.php/operation-announcement/op-a/op-a-01/1557-5-1-11-41-dfa4-t1



[障礙解除]5/1 11:41 亞太DFA4及T1光纜斷線，影響台北區網對外網路服務，目前正在搶修中。

作者 TANet NOC

DFA4及T1光纜已於13:32恢復。

==========

DFA4光纜斷線影響以下電路:

TA_TP_NTU_HUN-1、

TA_TP_NCU_HUN-1、

TA_TP_NCTU_HUN-1、

TA_TP_NTHU_HUN-1。

T1光纜斷線影響以下電路:

TA_TP1_SINICA_HUN-1

TA_TP2_SINICA_HUN-2

TA_TP1_TRTC_HUN-1

TA_TP2_TRTC_HUN-2

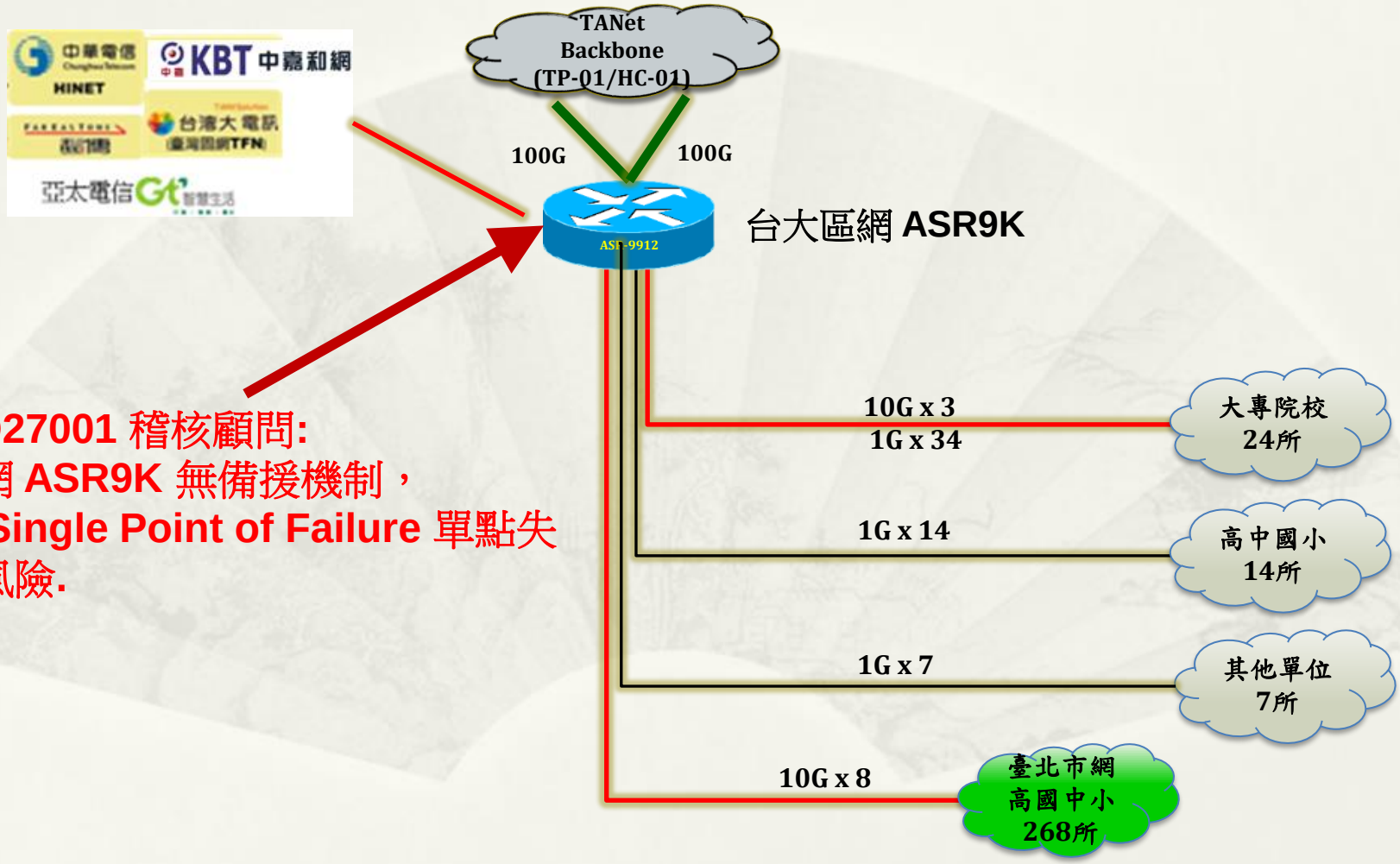
TA_TRTC_NCKU_10G-1

其中因台北區網< >新竹主節點的備援電路因先前新竹主節點100G卡板故障已中斷，目前DFA4光纜斷線又影響台北區網< >台北主節點電路，導致目前台北區網電路雙斷，影響台北區網TANet對外網路服務，目前正在搶修中。

Lesson Learns 與改善建議

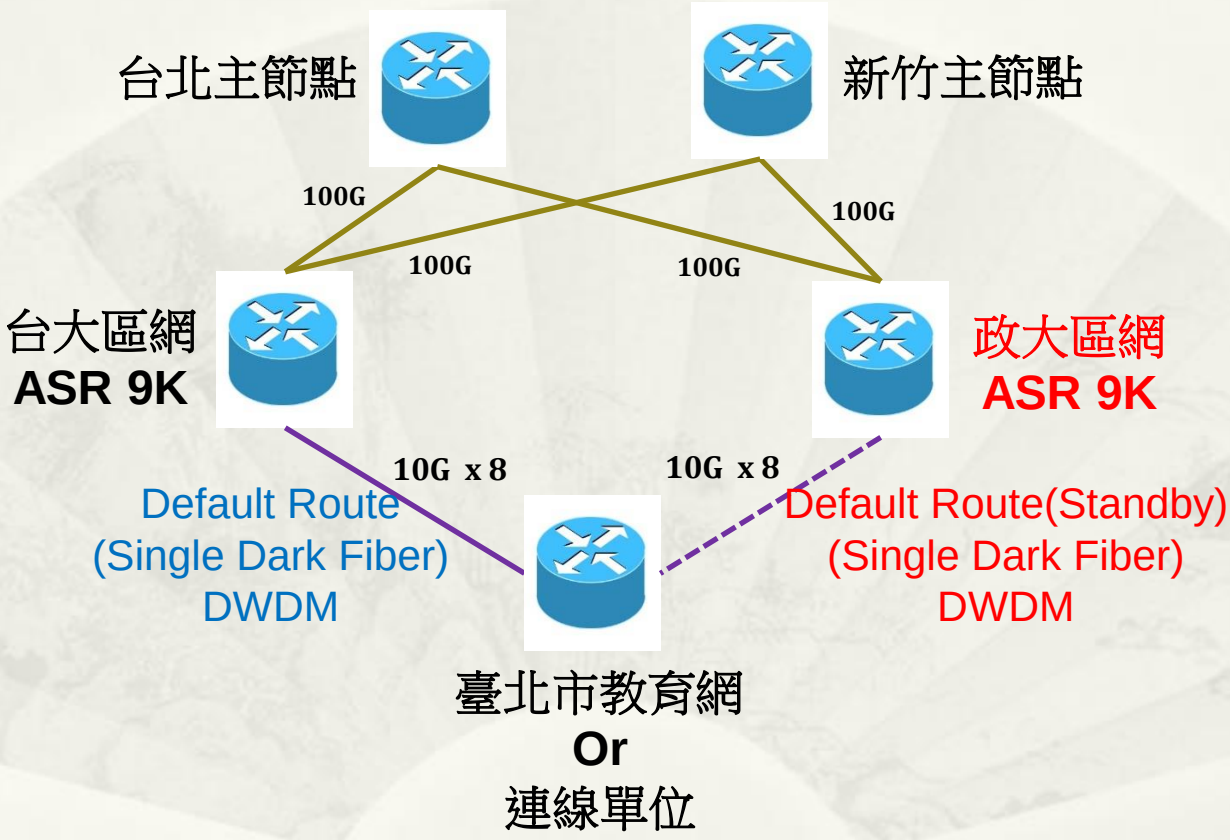
- 100G骨幹重要設備應有維護合約
  - 2022 ~ 2023/06 數月無維護合約
  - 2023/06/06: 華電聯網為 TANet 100G 新維護廠商
- Peer 電路應有 SLA 合約與斷線罰款機制
- TANet 骨幹應有24Hr 維運工程師
  - 異常通報與聯繫
  - TANet NOC 網站公告障礙與處理進度
- 建立其他區網備援機制，解決單點失效風險

台北區網 I
存在單點失效風險



ISO27001 稽核顧問:
區網 ASR9K 無備援機制，具 Single Point of Failure 單點失效風險.

建立其他區網備援機制
解決單點失效風險



建立其他區網備援機制
連線單位-內對外路由設定

- 兩筆 Default Route 使用 Administrative Distance 區分為 Active/Standby 各自指向 台大/政大 區網
- 使用 SLA ping 監控 台大區網 Peer IP，當失效時自動切換走政大區網
- Cisco 設定指令參考
  - ip sla 10
  - icmp-echo <台北主節點 peer ip> source-ip <市網peer ip>
  - ip sla schedule 10 life forever start-time now
  - track 1 ip sla 10 reachability

  - ip route 0.0.0.0 0.0.0.0 台大區網 peer ip track 1
  - ip route 0.0.0.0 0.0.0.0 政大區網 peer ip <AD>

建立其他區網備援機制
連線單位-外對內路由設定

- 政大區網使用 BGP AS-Path Prepend 降低教網(連線單位)網段 放給 台北/新竹之 路由優先權
- Cisco 設定指令參考
  - 政大區網 To 臺北主節點
    - xx.xx.xx.xx/16(市網網段) prepend as-path 1659
    - …
  - 政大區網 To 新竹主節點
    - xx.xx.xx.xx/16(市網網段) prepend as-path 1659
    - …

3.資安服務
109~112年度資安事件統計

	109	110	111	112
1、2級資安事件處理				
通報平均時數	0.04 小時	0.05 小時	0.001 小時	0.07 小時
應變處理平均時數	0.05 小時	0.86 小時	0.086 小時	0.25 小時
事件處理平均時數	0.74 小時	1.42 小時	0.087 小時	2.88 小時
通報完成率	100 %	99.89 %	100 %	100 %
事件完成率	100%	100%	94.48%	100%
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	1.12小時	0.55小時	0.003小時	0.83小時
資料更新完整校數	97.04%	100%	56.52%	100%

評審委員: 資事件完成率及資訊完整度，建議改善之。

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。

4. 特色服務
使用 ELK Stack 大數據分析異常事件

- 學網史上最大規模 DDoS 攻擊事件
- 快速緩解連線學校遭受 DDoS 攻擊
- 分析連線學校異常流量
  - 印表機使用 Public IP 且未設定存取控制

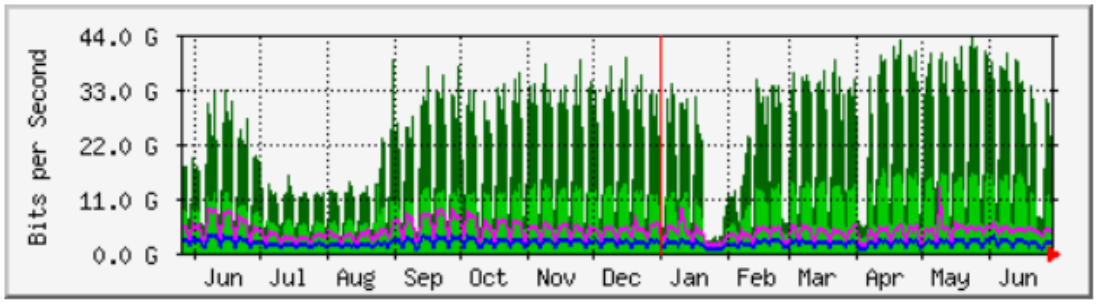
學網史上最大規模 DDoS 攻擊事件

攻擊資料匯總

- 攻擊方法: SYN Flood
- 攻擊期間: 4/20 ~ 5/15 (幾乎每天都有)
- 持續時間: 5分鐘~ 1小時
- 攻擊來源: 3 Subnets(/24)
  - 89.248.163.0/24、89.248.165.0/24、92.63.196.0/24
- 攻擊目的:
  - TANet 全網段，/24 網段輪流: 每次 1 ~ 3 分鐘
- 攻擊目的 Port: Random

TANet 100G 臺北主節點
攻擊期間: 4/20 ~ 5/15

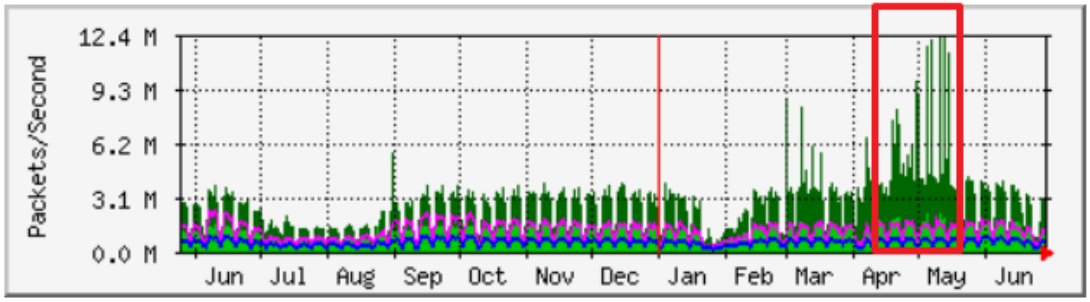
`Yearly' Graph (1 Day Average) 流量 bits per-second



	Max	Average	Current
台北主節點 => 北區區網	43.8 Gb/s (43.8%)	8850.3 Mb/s (8.9%)	11.5 Gb/s (11.5%)
北區區網 => 台北主節點	13.1 Gb/s (13.1%)	1845.4 Mb/s (1.8%)	2116.3 Mb/s (2.1%)

流量圖
無法顯示異常

`Yearly' Graph (1 Day Average) 封包數 packets per-second

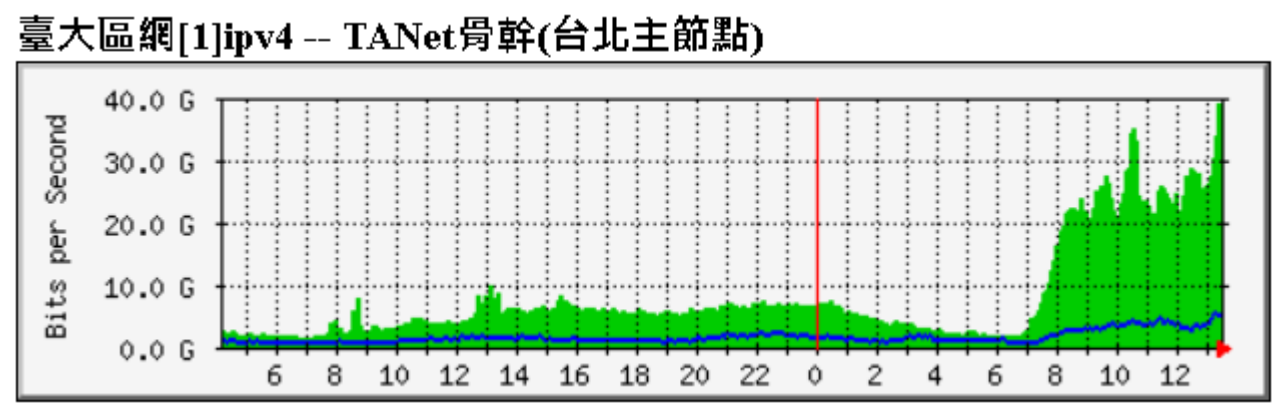


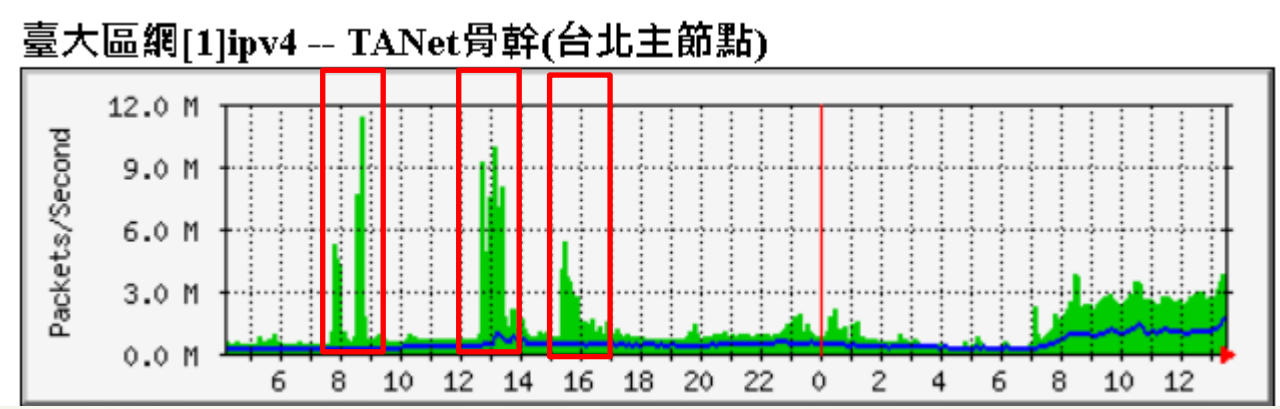
	Max	Average	Current
In 封包數, Packets	12.4 Mpkt/sec	1043.3 kpkt/sec	1132.8 kpkt/sec
Out 封包數, Packets	2292.3 kpkt/sec	488.3 kpkt/sec	469.2 kpkt/sec

臺灣大學

NTU National Taiwan University

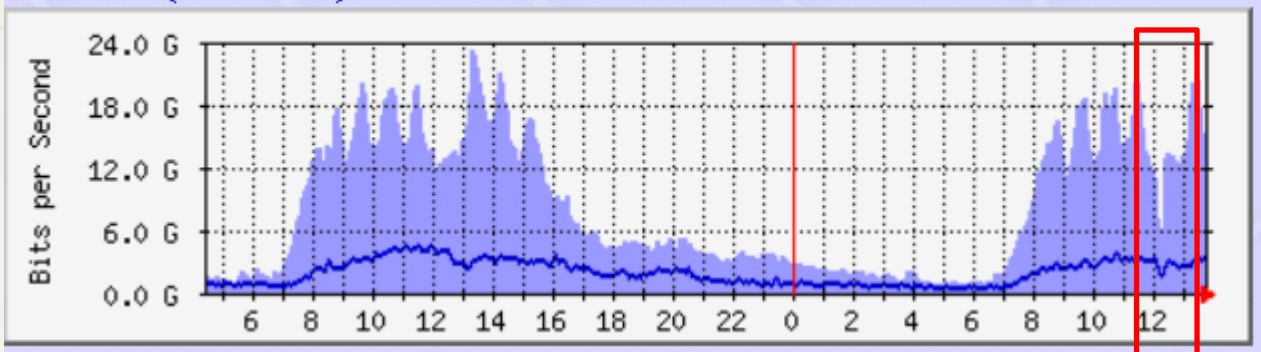
5/14 假日持續進行攻擊



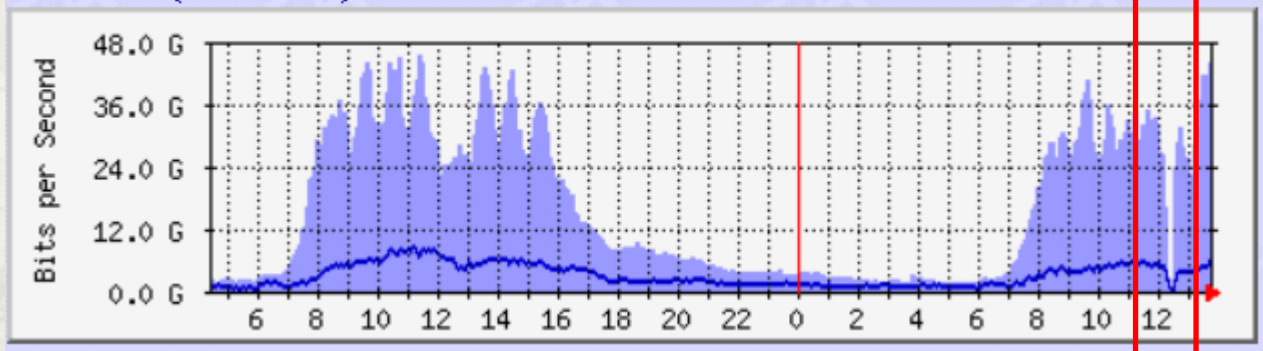


其他區網遭受攻擊

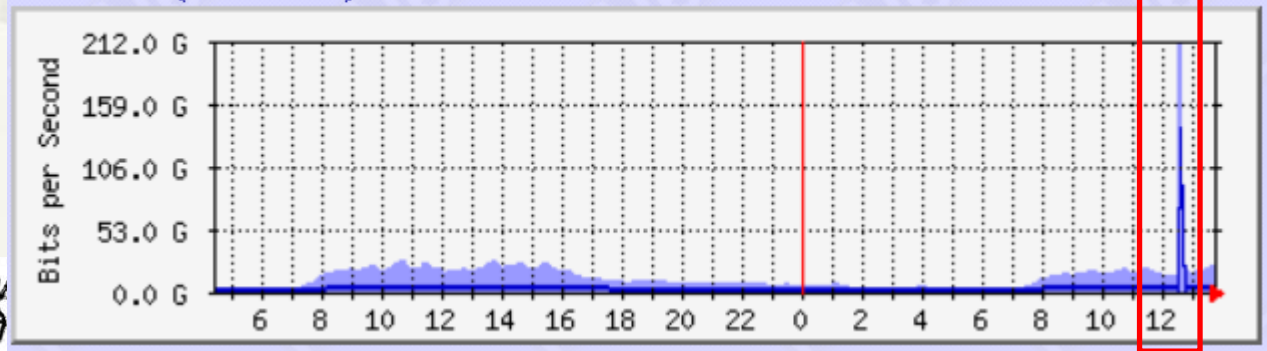
竹苗區網(陽明交大) --- 主節點



台中區網(中興大學) --- 主節點

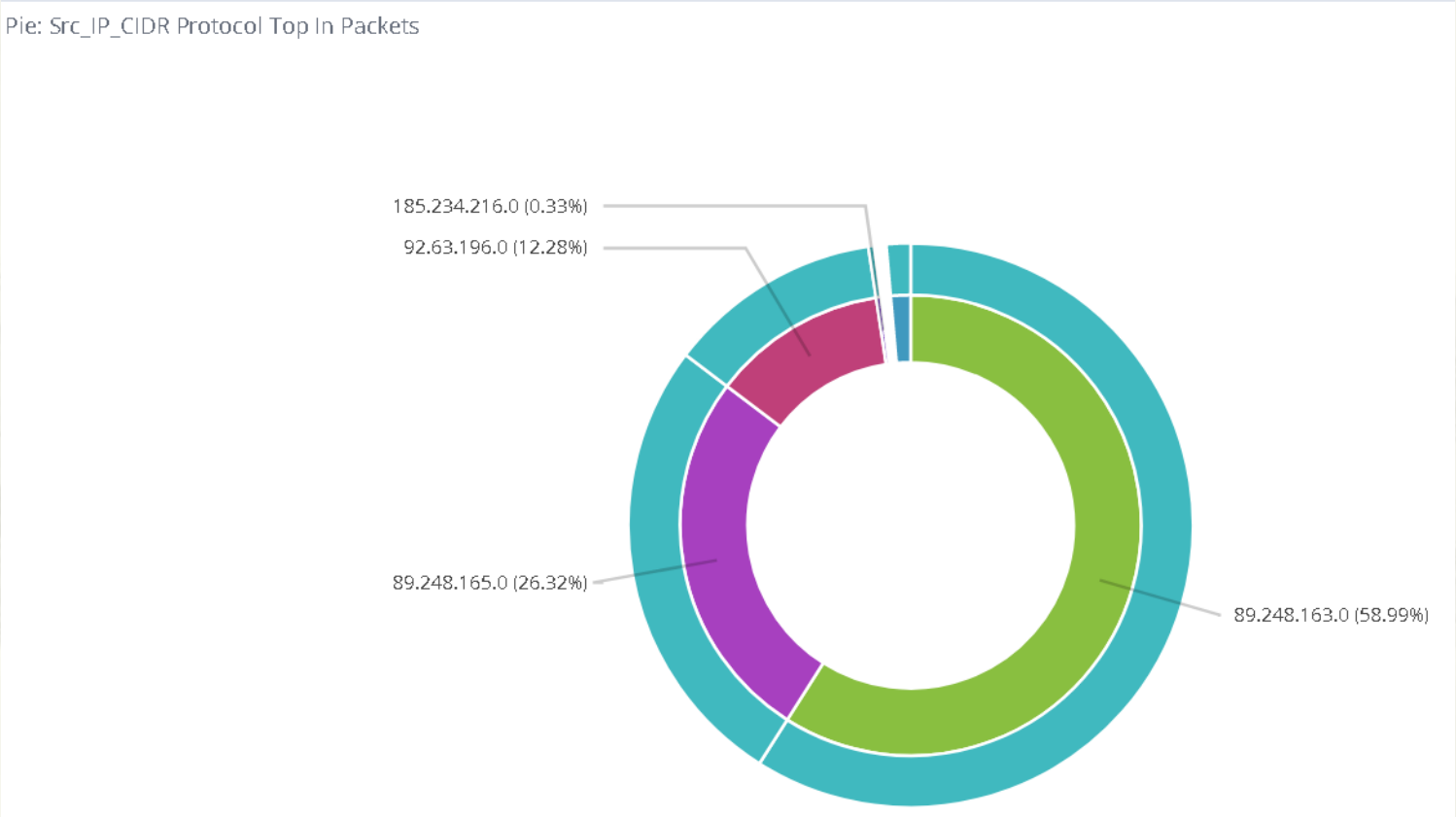


台南區網(成功大學) --- 主節點

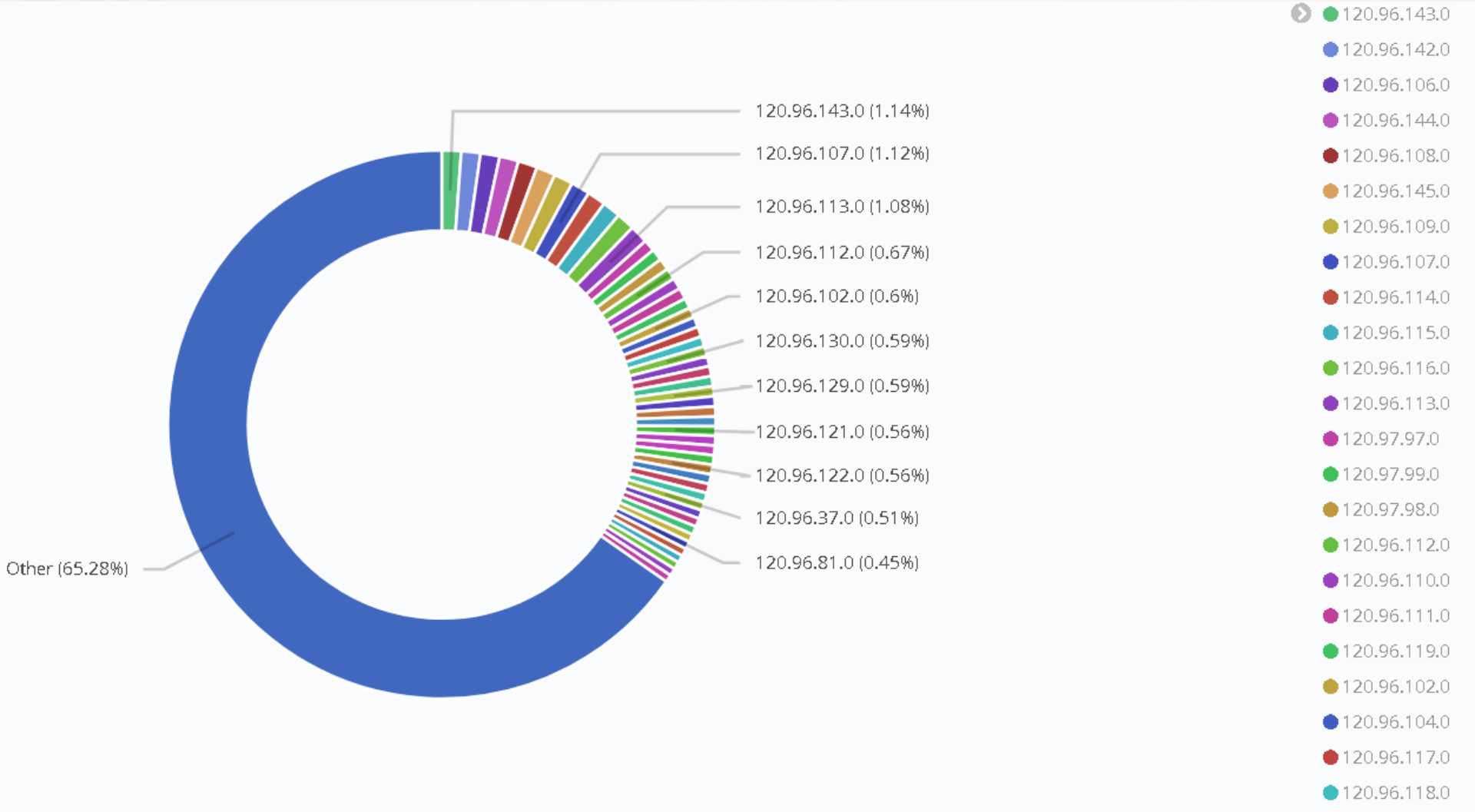


攻擊來源 IP CIDR /24

* 89.248.163.0/24、89.248.165.0/24、92.63.196.0/24

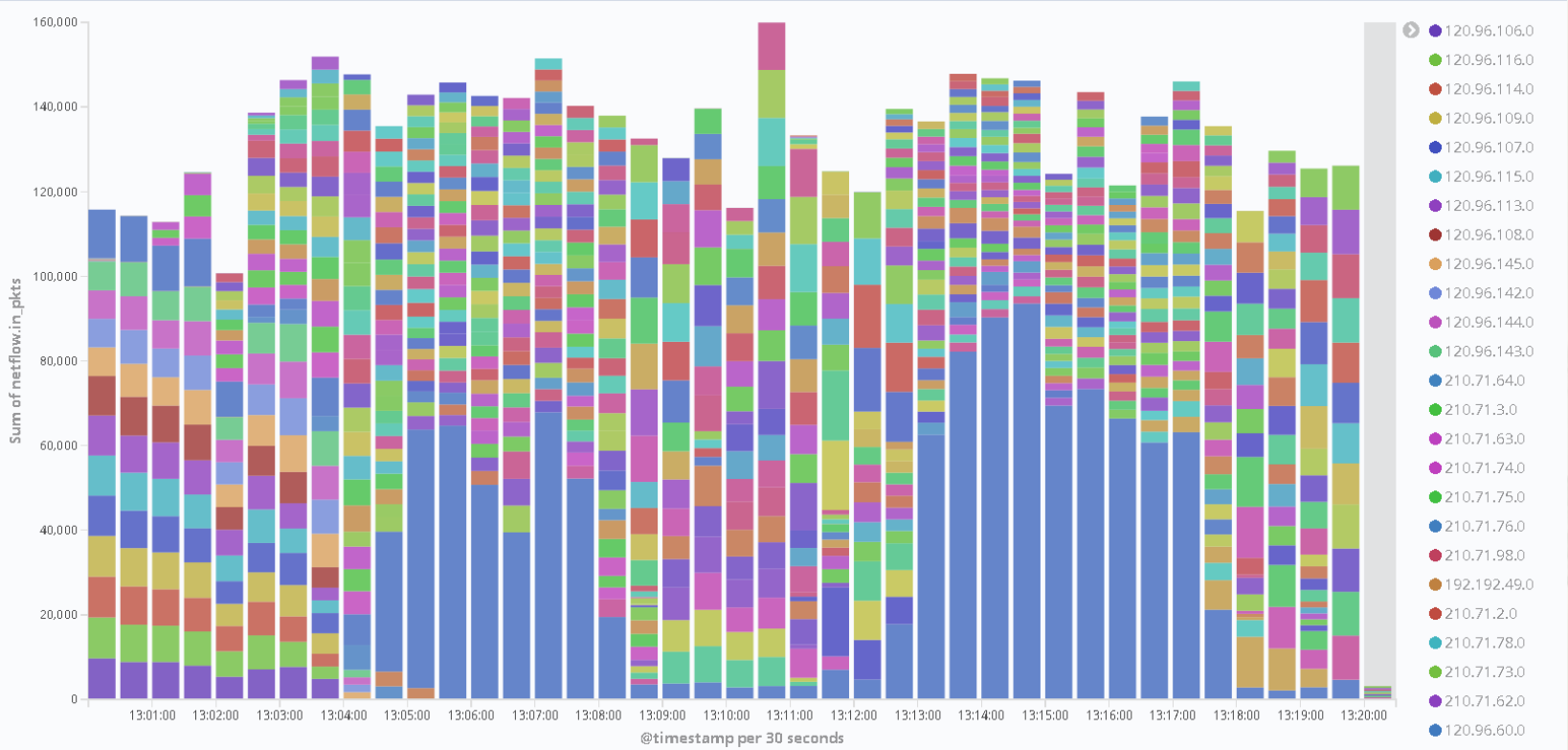


攻擊目的 IP CIDR /24

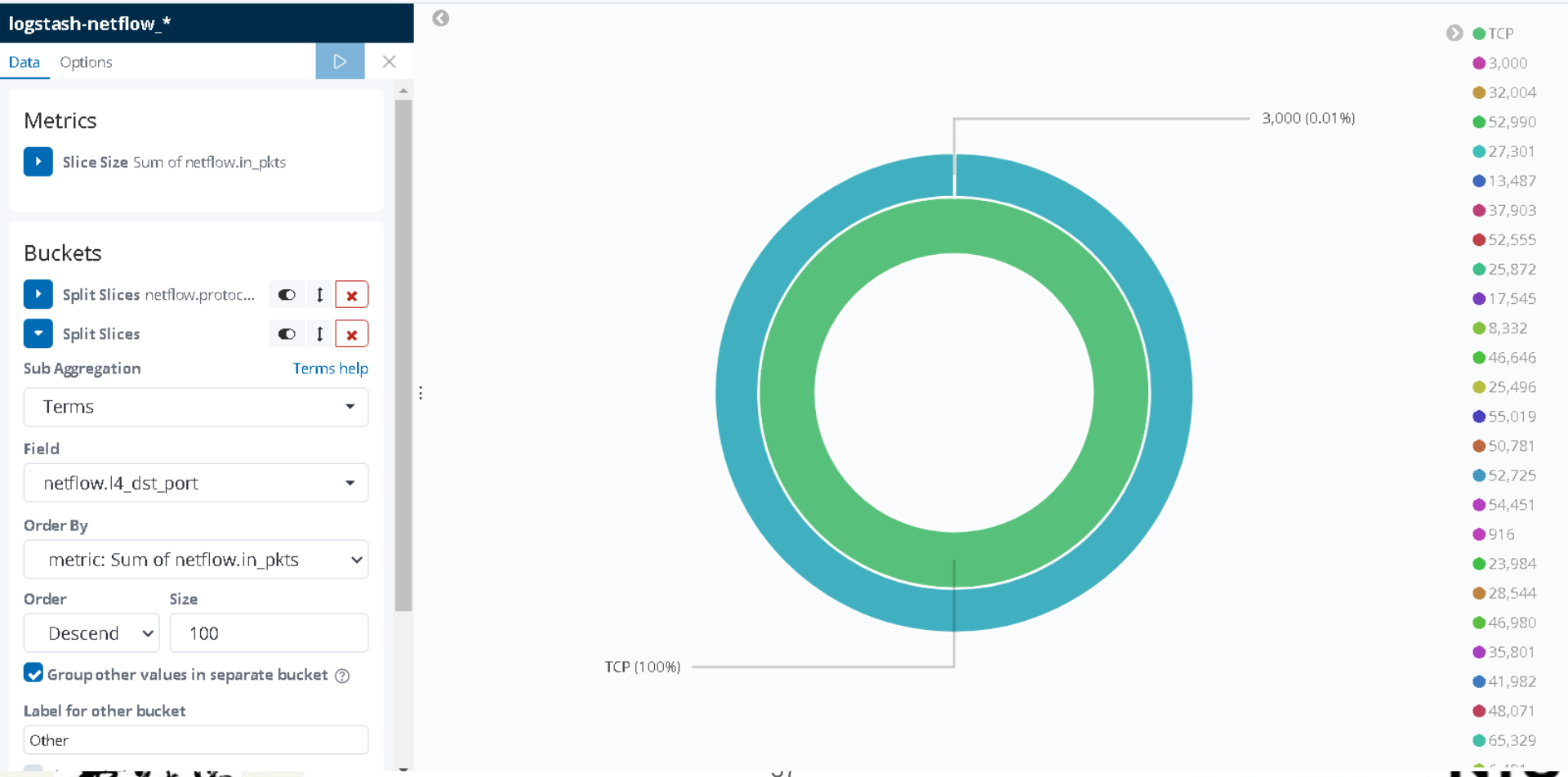


攻擊目的 IP CIDR /24

* Class C網段輪流: 每次 1 ~ 3 分鐘



Destination Port Top100 (Random)



阻擋方法

- DDoS 導流清洗(Out of Band)
  - 將攻擊”來源 IP” 導入流量清洗
  - ※過去皆是導流”目的 IP”
- Router 用 ACL 將攻擊來源 IP 封包 Drop
  - ACL 設定於區網端 100G 介面 In
  - ACL 設定於 TANet Border Router 介面 In
- Router 用ACL 將攻擊來源 AS 所有 IP 網段封包 Drop
  - 於 TANet Border Router 介面 In
  - 教育部駐點工程師採用此方式

2023/05/15 16:00
將攻擊來源 AS 所有 IP 網段封包 Drop

快速緩解連線學校遭受 DDoS 攻擊事件

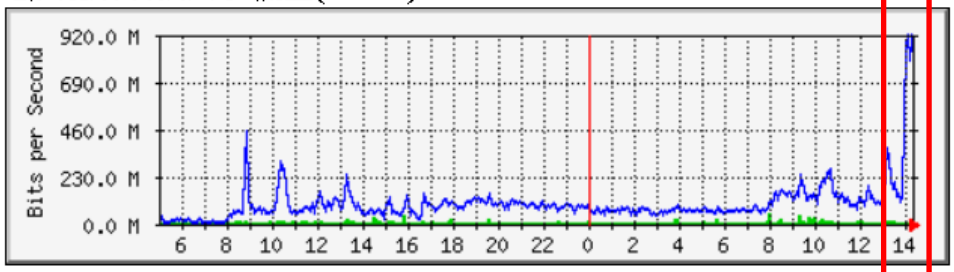
2023/09/23 14:00

收到告警、ELK 分析、進行導流
僅花費 9 分鐘時間

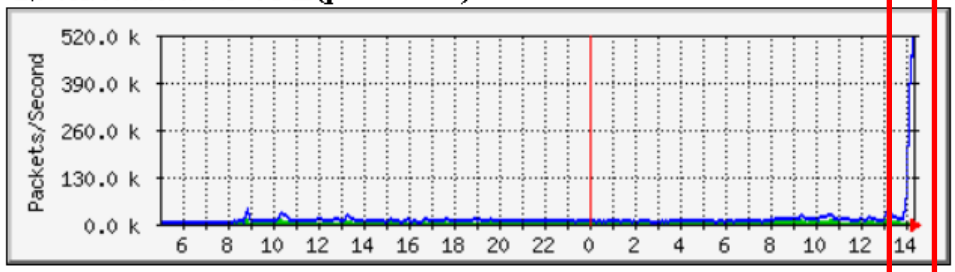
* 14:03 通報網路發生異常
* **14:08** 回覆遭受 DDoS 攻擊，使用 ELK Stake 分析
* 14:13 完成 DDoS 來源與攻擊目標分析，通知 A-SOC
* **14:17** A-SOC 完成導流清洗

MRTG 流量與封包圖

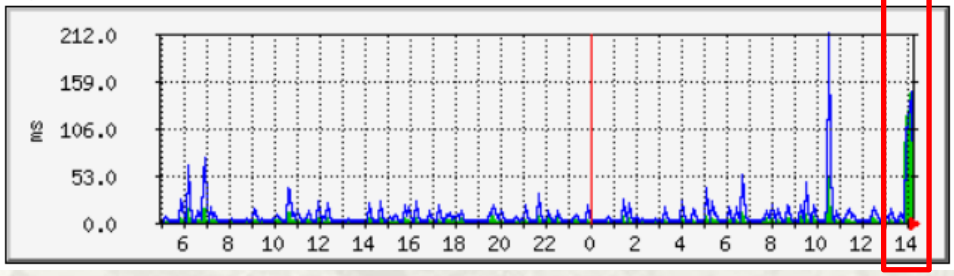
宏國德霖科技大學 流量(bit/sec)



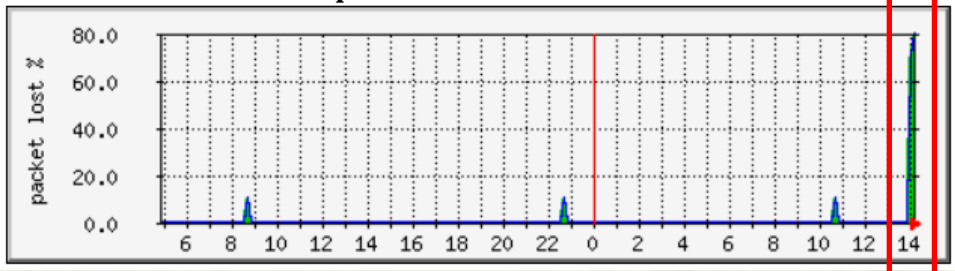
宏國德霖科技大學 封包(packet/sec)



宏國德霖科技大學 PING



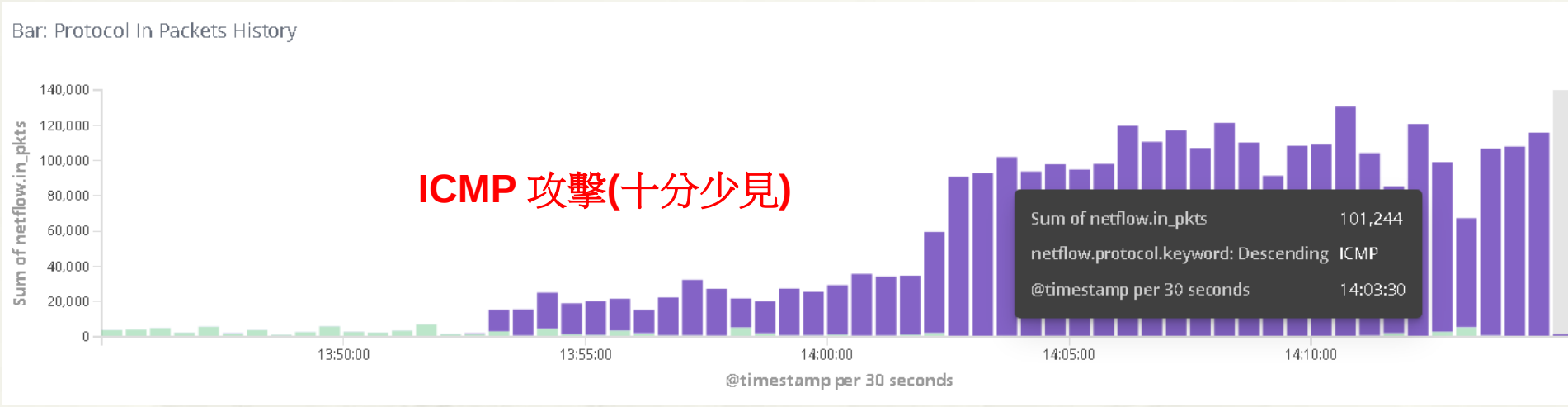
宏國德霖科技大學 PING packet lost %

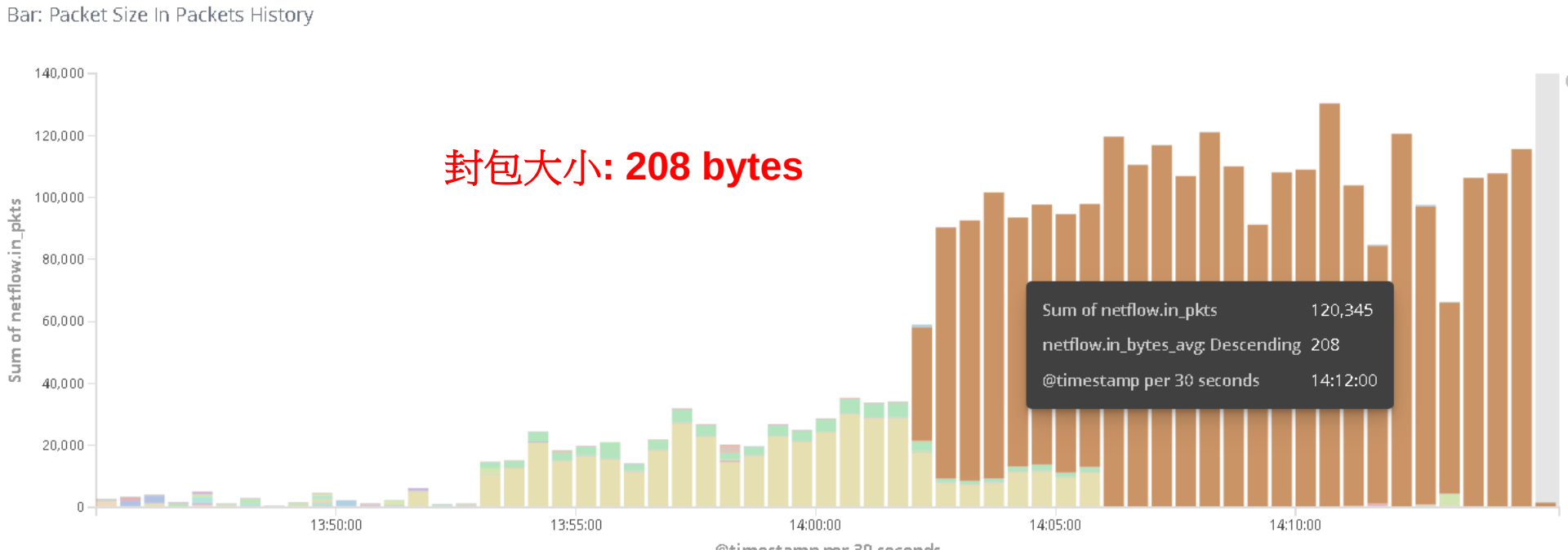


DDoS 流量清洗


Concurrent Connections
Concurrent Connections
Max 3 K
23.Sep.2023 14:19
Min 1
23.Sep.2023 14:06
4 K
3 K
2 K
1 K
0
Concurrent Connections
14:05 14:06 14:07 14:08 14:09 14:10 14:11 14:12 14:13 14:14 14:15 14:16 14:17 14:18 14:19
Traffic Bandwidth
bps
pps
Inbound
Outbound
Received
Max 1.9 G
23.Sep.2023 14:19
Min 0
23.Sep.2023 14:05
Dropped
More..
2 G
1.5 G
1 G
500 M
0
Bits/Sec
14:05 14:06 14:07 14:08 14:09 14:10 14:11 14:12 14:13 14:14 14:15 14:16 14:17 14:18

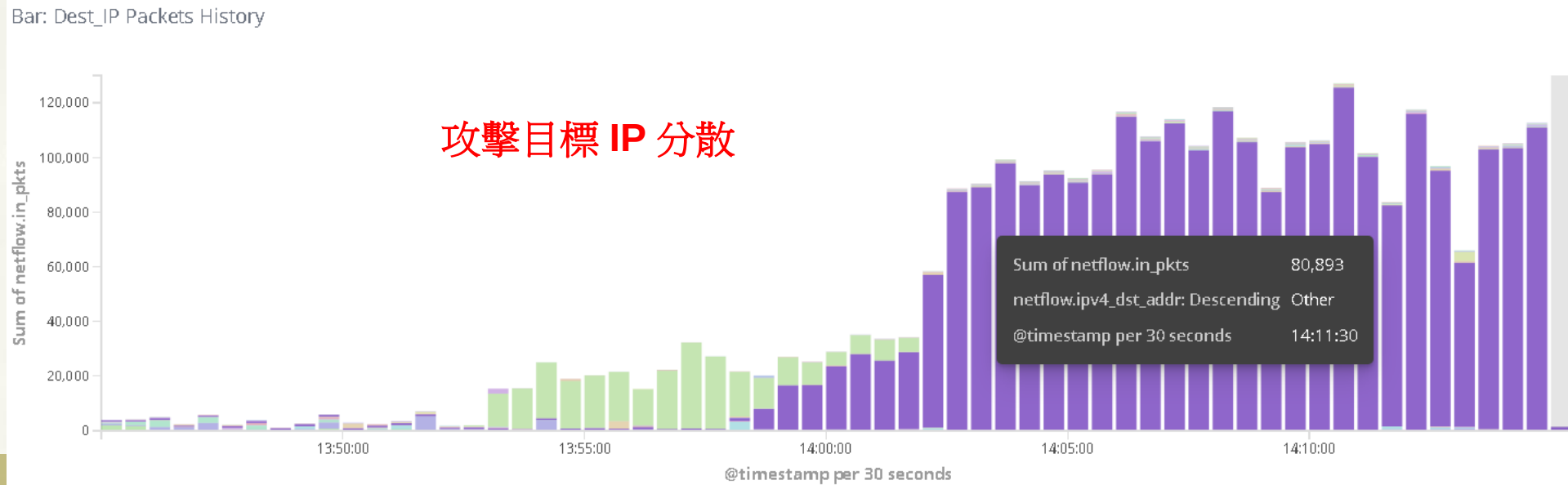
攻擊協定 與 Packet Size



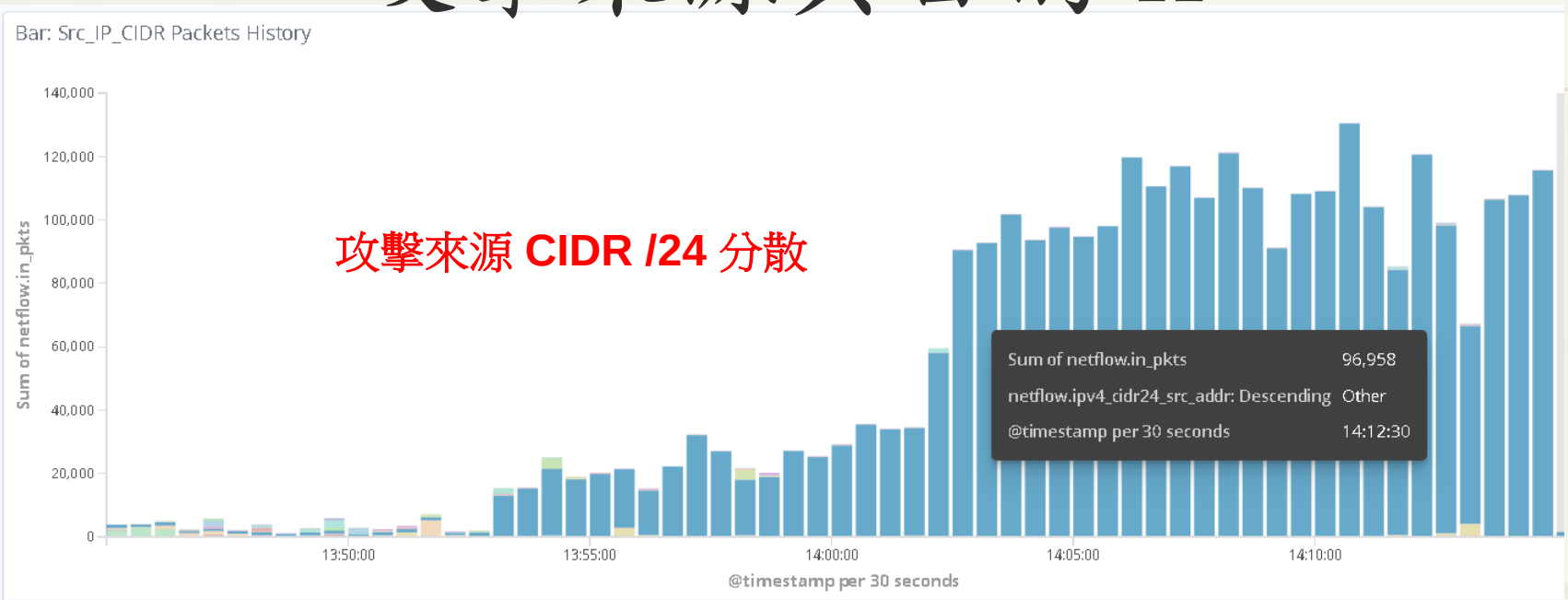


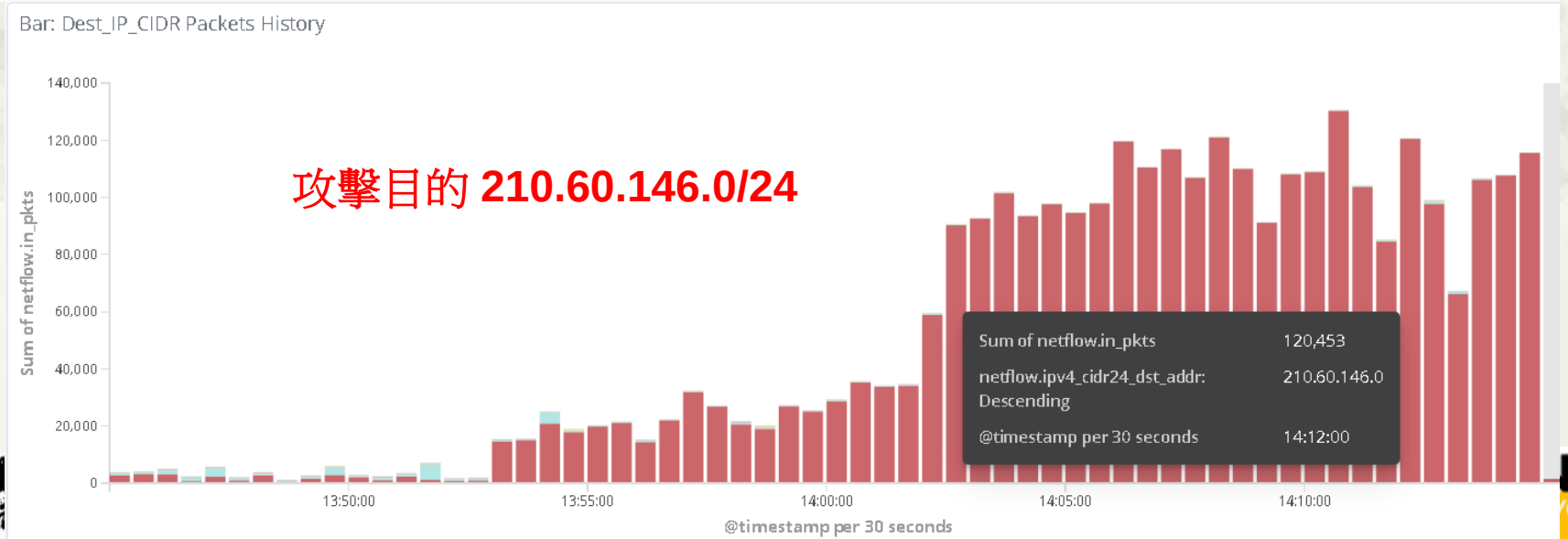
攻擊來源與目的 IP


Bar: Source_IP Packets History
September 23rd 2023, 13:45:00.000 to September 23rd 2023, 14:15:00.000
host.keyword: "192.192.60.112"
netflow.output_snmp: "159"
攻擊來源 IP 分散
Sum of netflow.in_pkts 93,555
netflow.ipv4_src_addr: Descending Other
@timestamp per 30 seconds 14:04:00
Sum of netflow.in_pkts
140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
13:50:00
13:55:00
14:00:00
14:05:00
14:10:00
@timestamp per 30 seconds


Bar: Dest_IP Packets History
攻擊目標 IP 分散
Sum of netflow.in_pkts 80,893
netflow.ipv4_dst_addr: Descending Other
@timestamp per 30 seconds 14:11:30
Sum of netflow.in_pkts
120,000
100,000
80,000
60,000
40,000
20,000
0
13:50:00
13:55:00
14:00:00
14:05:00
14:10:00
@timestamp per 30 seconds

攻擊來源與目的 IP


Bar: Src_IP_CIDR Packets History
Sum of netflow.in_pkts
140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
13:50:00
13:55:00
14:00:00
14:05:00
14:10:00
@timestamp per 30 seconds
攻擊來源 CIDR /24 分散
Sum of netflow.in_pkts 96,958
netflow.ipv4_cidr24_src_addr: Descending Other
@timestamp per 30 seconds 14:12:30

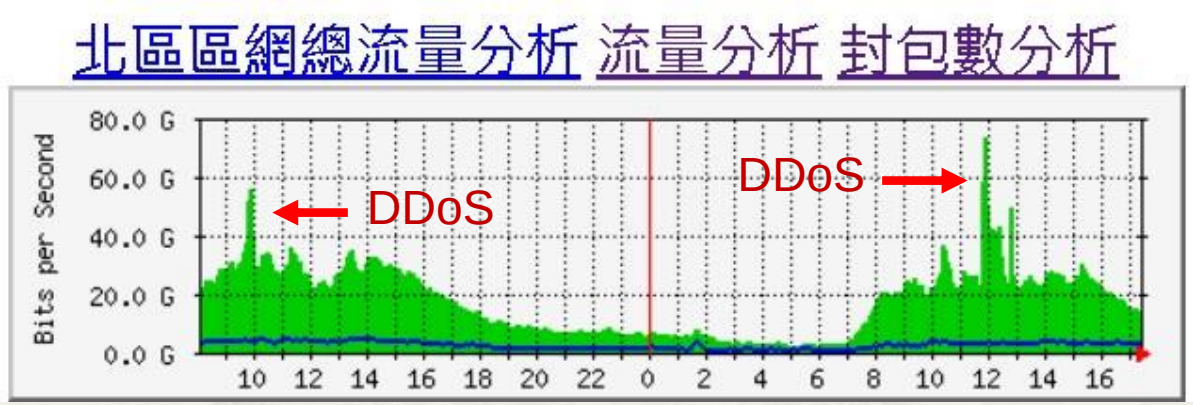

Bar: Dest_IP_CIDR Packets History
Sum of netflow.in_pkts
140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
13:50:00
13:55:00
14:00:00
14:05:00
14:10:00
@timestamp per 30 seconds
攻擊目的 210.60.146.0/24
Sum of netflow.in_pkts 120,453
netflow.ipv4_cidr24_dst_addr: Descending 210.60.146.0
@timestamp per 30 seconds 14:12:00

DDoS 通報(事後補填)

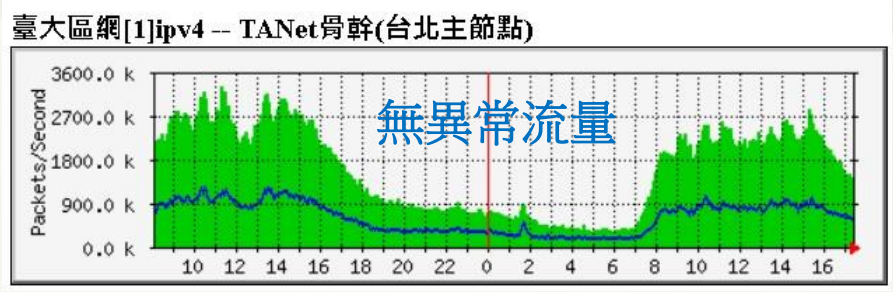
無 ICMP 選項 →

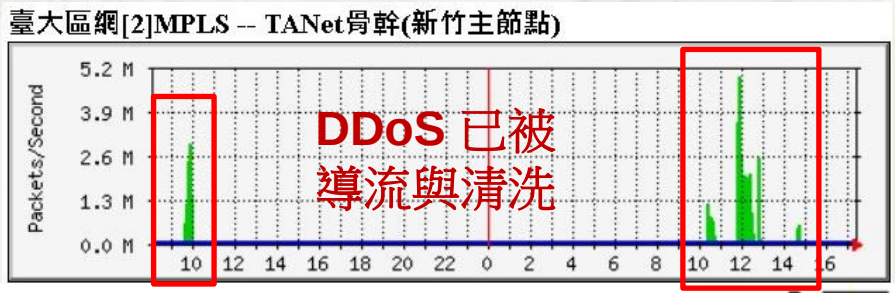
補充: DDoS 清洗成效
2023/09/01 大安高工 DDoS 事件

* **尚未導入**清洗



* **順利導入**清洗



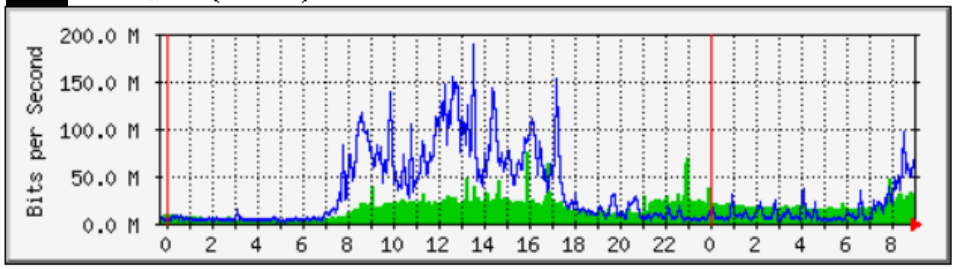


分析連線學校異常流量

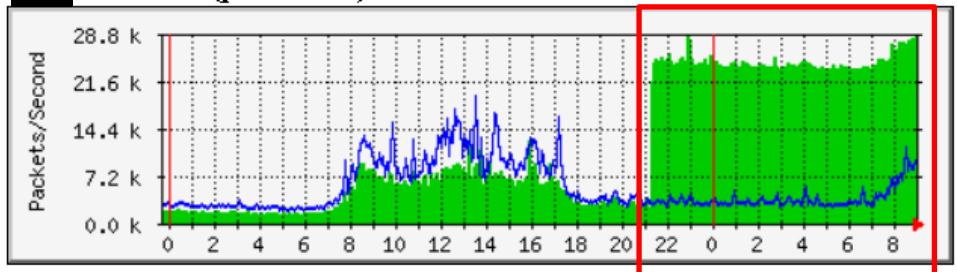
印表機使用 Public IP
且未設定存取控制

XX大學 2023/09/11
內對外封包數異常增加

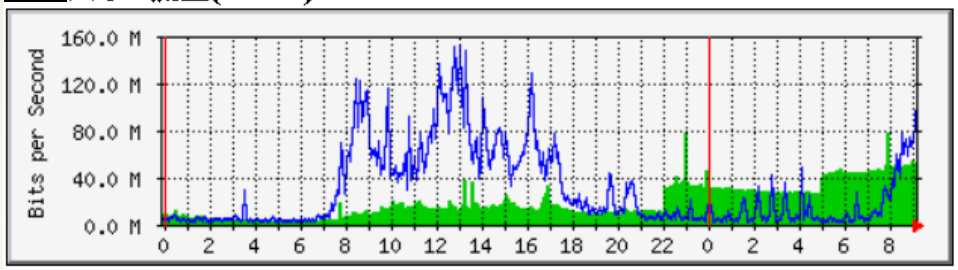
大學1 流量(bit/sec)



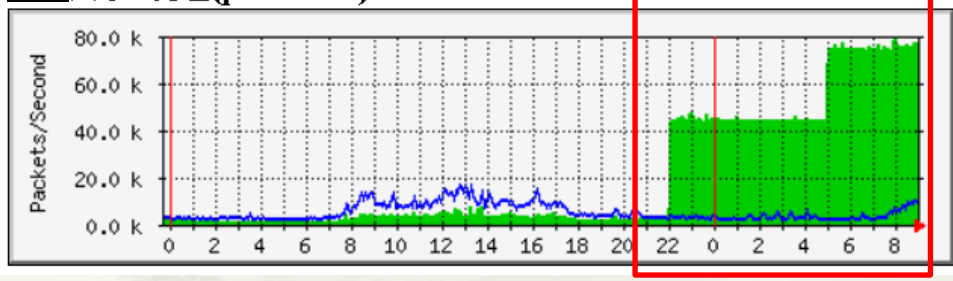
大學1 封包(packet/sec)



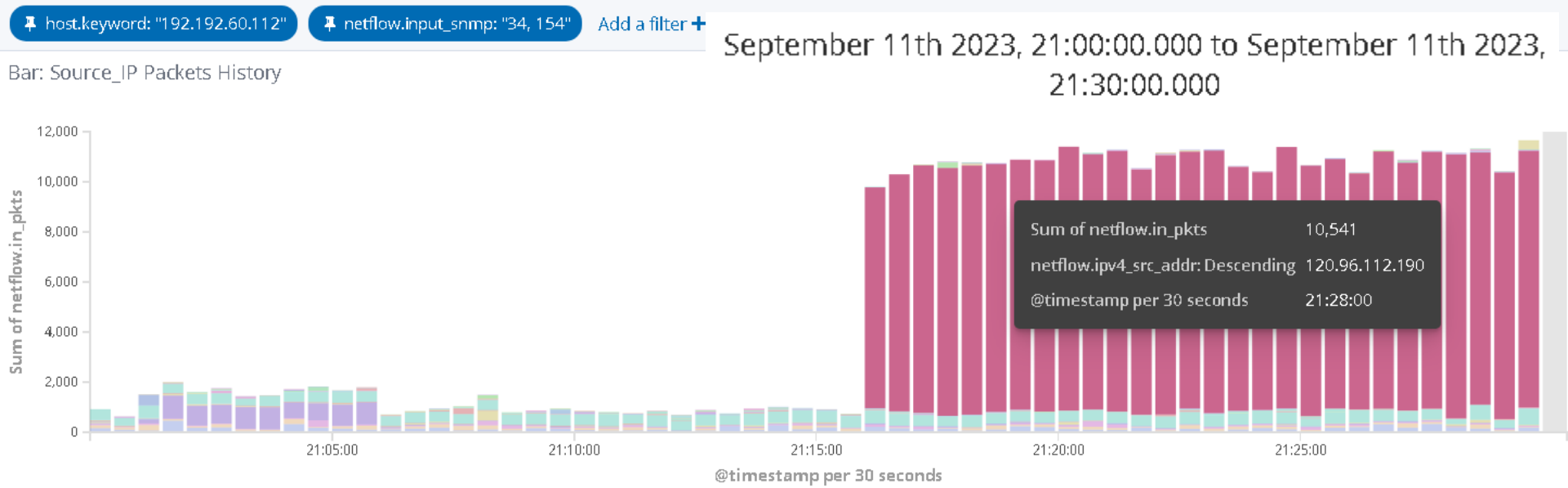
大學2 流量(bit/sec)

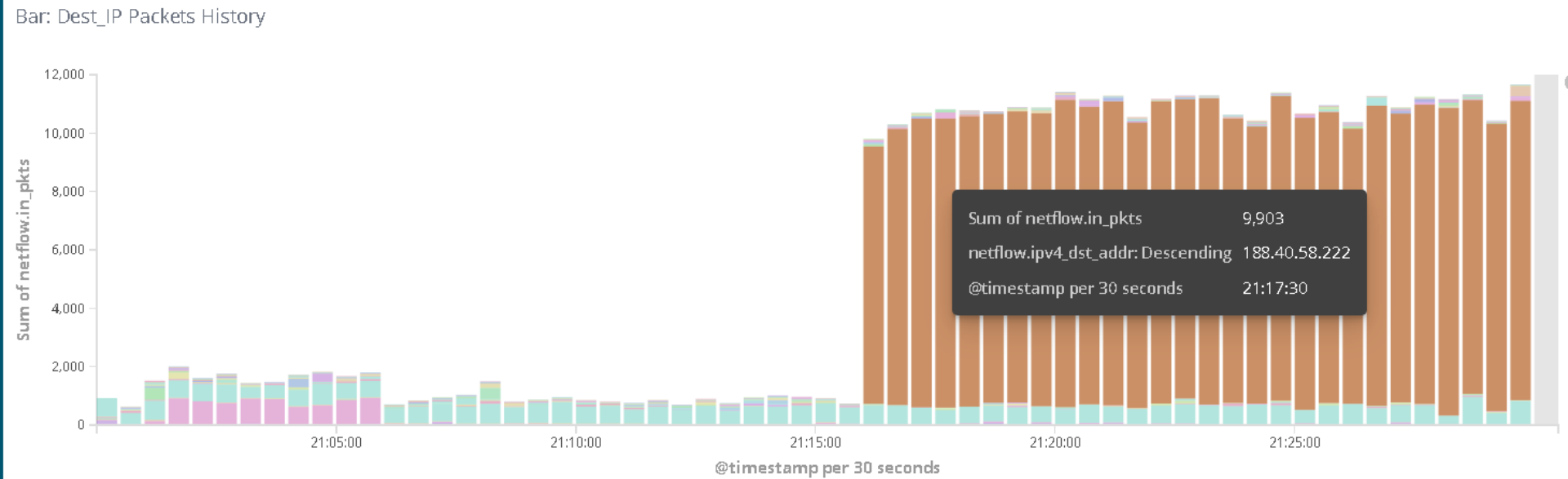


大學2 封包(packet/sec)



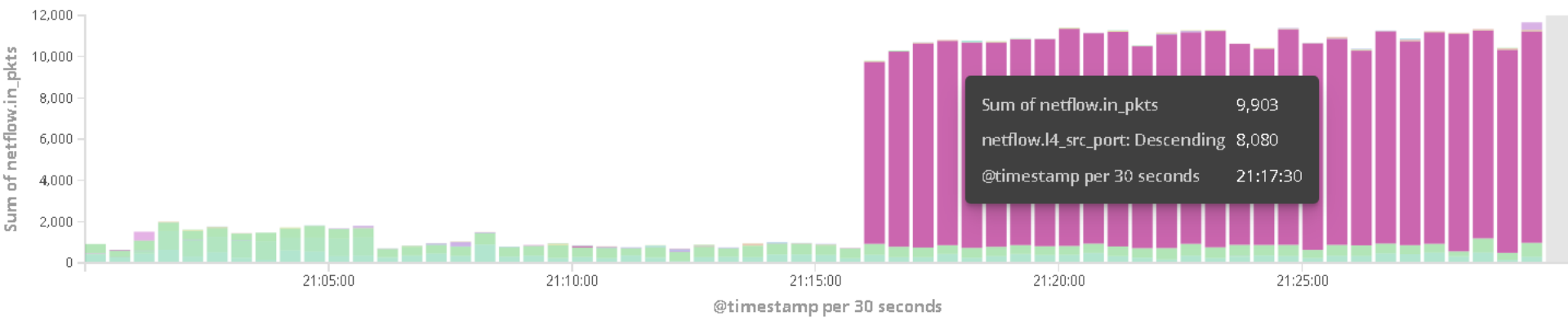
來源與目的 IP


host.keyword: "192.192.60.112"
netflow.input_snmp: "34, 154"
Add a filter +
September 11th 2023, 21:00:00.000 to September 11th 2023, 21:30:00.000
Bar: Source_IP Packets History
Sum of netflow.in_pkts
12,000
10,000
8,000
6,000
4,000
2,000
0
21:05:00
21:10:00
21:15:00
21:20:00
21:25:00
@timestamp per 30 seconds
Sum of netflow.in_pkts 10,541
netflow.ipv4_src_addr: Descending 120.96.112.190
@timestamp per 30 seconds 21:28:00

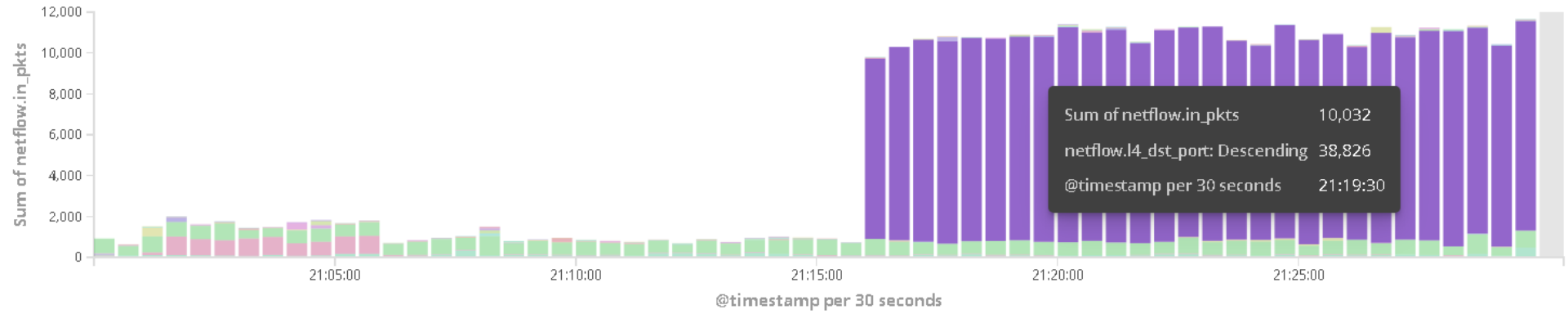

Bar: Dest_IP Packets History
Sum of netflow.in_pkts
12,000
10,000
8,000
6,000
4,000
2,000
0
21:05:00
21:10:00
21:15:00
21:20:00
21:25:00
@timestamp per 30 seconds
Sum of netflow.in_pkts 9,903
netflow.ipv4_dst_addr: Descending 188.40.58.222
@timestamp per 30 seconds 21:17:30

Source/Destination Port

Bar: Source Port In Packets

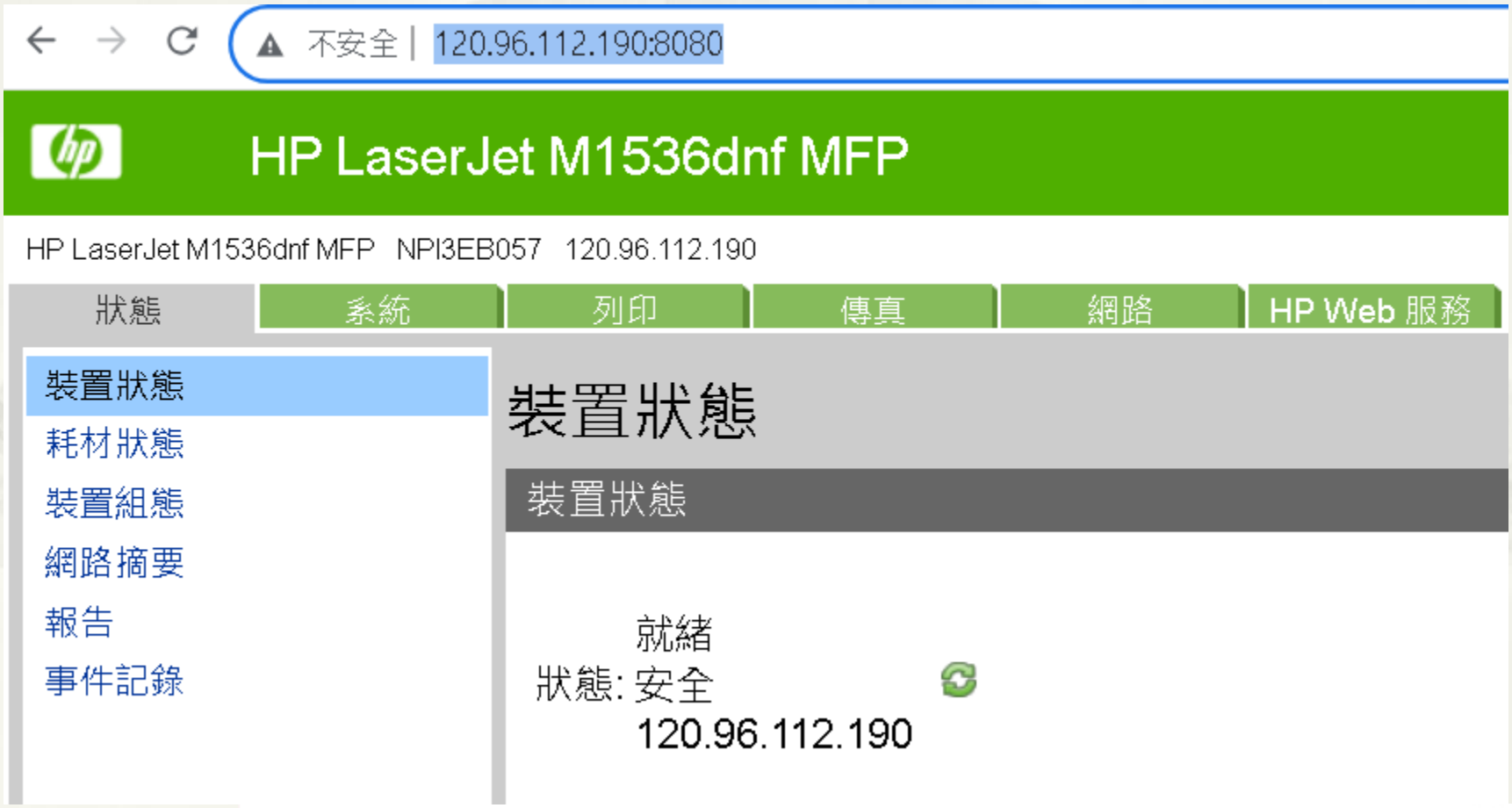


Bar: Dest_Port Packets History



印表機使用 Public IP 且未設定存取控制

* http://120.96.112.190:8080/



5.成效精進

111年評審委員建議與回覆

No	委員建議	回覆
1	經費達成率偏低因人員離職影響，建議學校挹注配合款，可提升攬才留才以利業務推展。	針對技術人員薪資之補助，目前已有使用其他計畫之結餘款或其他計畫仍有餘裕之部分進行補助。
2	加強技術分享、交流擴散或降低TANet 維運相關問題。	於下列時間地點與其他區網進行技術分享與交流: 2022/12 台北區網 I 區網會議: 窮人版WAF: ModSecurity(Open Source WAF) 2023/06 台東區網暑期課程(台東大學): HTTPS 憑證簽署原理與實做 2023/08 高屏澎暑期課程(中山大學): Reverse Proxy 運作原理與實做:以 NGINX 為例 2023/10 高屏澎區網會議(中山大學): NGINX Load Balance 實做、窮人版WAF: ModSecurity 實做

111年評審委員建議與回覆

No	委員建議	回覆
3	計畫目標網路妥善率 99.9%，建議明確目標延伸至小數點下 2 位數。	因發生非區網所能控制之台北與新竹100G骨幹雙斷，合計斷線時間: 5小時6分鐘(306分鐘)，實際網路妥善率 96.51% 建議改善方法如下: 100G骨幹重要設備應有維護合約 Peer 電路斷線建議應有 SLA 合約與罰款機制 TANet 骨幹應有 24Hr 維運工程師，可負責異常通報與聯繫並 即時於 TANet NOC 網站公告障礙與處理進度 建立其他區網備援機制，解決單點失效風險
4	建議辦理每年區網連線學校基礎資料重新評核與審查。	預計於今年第二次區網會議(12月)辦理，需要更新的資訊包含: 聯絡人資訊、目前 Peer 電路廠商與租用頻寬、未來擴頻需求、IPv6導入與使用情形

111年評審委員建議與回覆

No	委員建議	回覆
5	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偏低建議改善。	已經有加強宣導與通知，今年資訊完整度已達 100%
6	資安事件處理，事件完成率 94.48%，資訊完整度為 56.52%，建議改善之。	已經有加強宣導與改善，今年事件完成率與資訊完整度已達 100%
7	建議協助尚無 ipv6 網段之連線單位申請 IPv6 及協助其連線：諸如大學入學考試中心、中華民國學生棒球運動聯盟、高中體育總會、國家地震中心等等。另外國中小的 IPv6 連線亦建議盡速完成。	本年度增加: 大專院校 + 1: 東吳大學 其他單位 + 1: 中央氣象局 尚無 ipv6 網段之連線單位，已經向教育部承辦人提出申請，目前正在請示長官後續辦理流程與步驟。

111年評審委員建議與回覆

No	委員建議	回覆
8	資安助理於 4/31 離職，至今尚未找到合適人選，為避免資安空窗期過久，中心人力負荷過重，建議未來應規畫相關人力遞補方案。	新任資安助理已於112年1月1日到職，因就業市場資安人力短缺，長官預計提高技術人員薪資，目前已使用其他計畫之結餘款或其他計畫仍有餘裕之部分進行補助。
9	本年雖已擬定各種異常斷線之 BCP 演練計畫，惟建議可於每次 BCP 演練時採複合式情境演練，可模擬多種狀況同時發生之應處作業，未來亦可降低事故發生時之處置時間。	今年五月實際發生台北與新竹主節點100G骨幹雙斷之情況，合計斷線時間: 5小時6分鐘(306分鐘)，檢討發生的原因為主節點卡版故障與 100G 電路異常，此兩項因素皆非區網所能控制，建議改善方法如下: 100G骨幹重要設備應有維護合約 Peer 電路斷線建議應有 SLA 合約與罰款機制 TANet 骨幹應有 24Hr 維運工程師，可負責異常通報與聯繫並 即時於 TANet NOC 網站公告障礙與處理進度 建立其他區網備援機制，解決單點失效風險

111年評審委員建議與回覆

No	委員建議	回覆
10	資安事件完成率較去年降低，僅為 99.48%，建議應了解原因及研擬如何提升資安事件完成率。	已經有加強宣導與改善，今年事件完成率已達 100%
11	區網中心辦理資安防護或弱掃服務(含諮詢)，建議可於明年執行複掃時使用其他弱掃工具，以強化弱點偵測之強度與廣度。	去年使用成大弱掃平台，該平台使用 Acunetix 軟體，今年因校內在評估購買網頁弱掃軟體，有同時比較 IBM AppScan、Burp Suite's Web Vulnerability Scanner、Acunetix 等三套軟體之掃描結果，詳見 6. 基礎維運: 網頁弱掃軟體測試。

6.基礎維運

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

v2.2

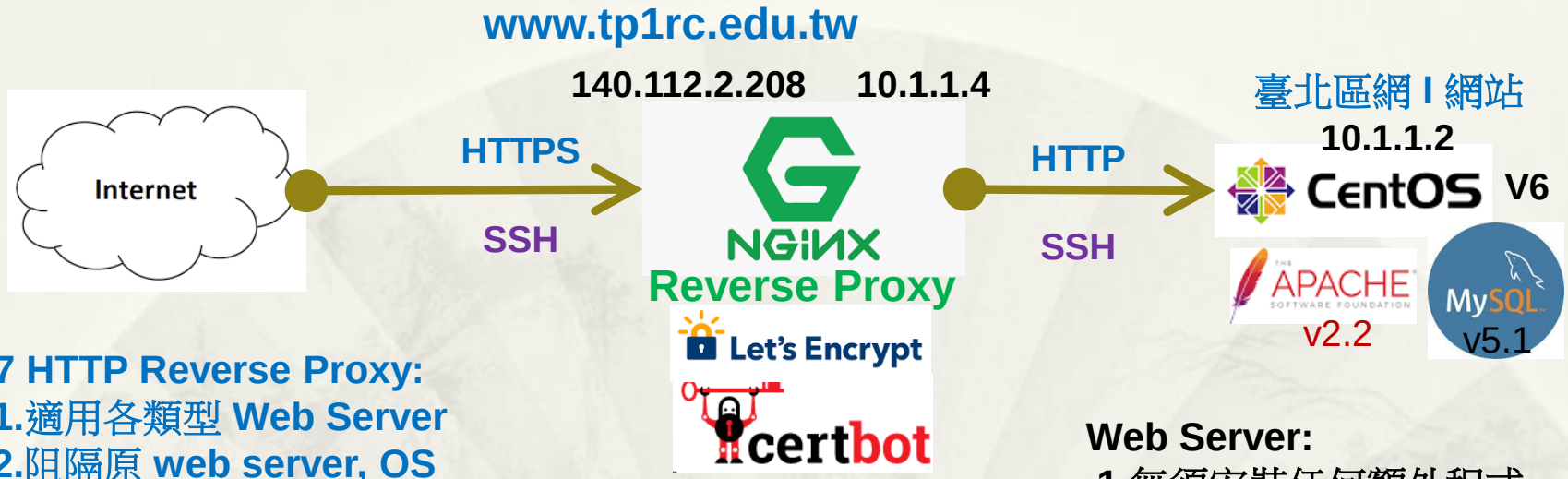
v5.1

- 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

網站安全
Web Site Security

* 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

區網網頁新架構



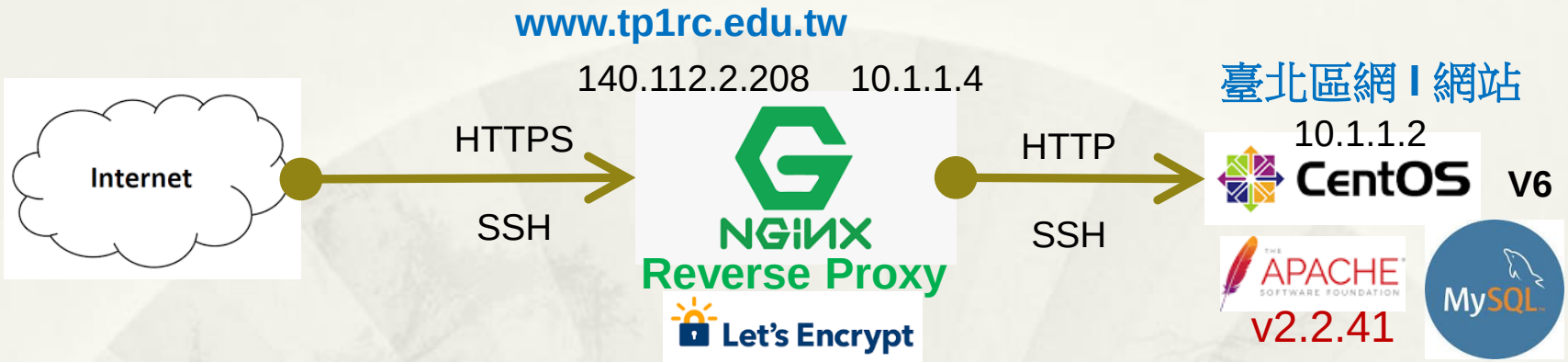
L7 HTTP Reverse Proxy:
1.適用各類型 Web Server
2.阻隔原 web server, OS 暴露於 Internet.
3.額外提供 Load Balance、Content Cache、WAF 功能.

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)

1. 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

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

區網弱掃報告
Medium Detail

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

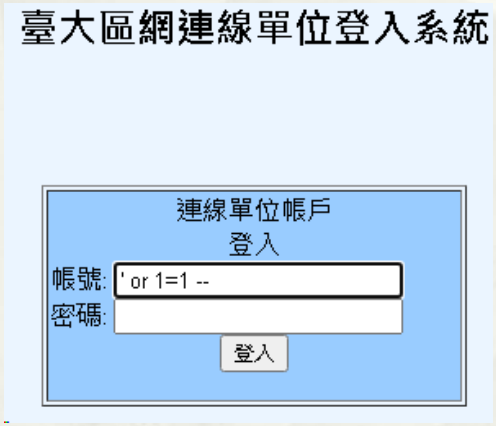
CVE-2011-3192 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192)
Apache HTTPD Security ADVISORY (http://mail-archives.apache.org/mod_mbox/httpd-announce/201108.mbox/%3C20110824161640.122D387DD@minotaur.apache.org%3E)
Apache httpd Remote Denial of Service (memory exhaustion) (https://www.exploit-db.com/exploits/17696)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

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

網站安全實做與推廣課程

* 2022/12 台北區網 I 區網會議
  * 窮人版WAF: ModSecurity(Open Source WAF)
* 2023/06 台東區網暑期課程(台東大學)
  * HTTPS 憑證簽署原理與實做
* 2023/08 高屏澎暑期課程(中山大學)
  * Reverse Proxy 運作原理與實做:以 NGINX 為例
* 2023/10 高屏澎區網會議(中山大學)
  * NGINX Load Balance 實做
  * 窮人版WAF: ModSecurity 實做

評審委員: 加強技術分享、交流擴散或降低 TANet 維運相關問題。

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

評審委員: 區網執行弱掃服務，建議可使用其他弱掃工具，以強化弱點偵測之強度與廣度。

7.對連線學校服務的支持度

* 1.網管經驗分享 IP 切網段
* 2.112年度區網暑期課程
* 3.區網網管會議
* 4.滿意度調查

網管經驗分享
IP 切網段

新增連線單位: 中央氣象局

新增連線單位: 中央氣象局 (原接教育部科技大樓)

* 原 IPv4 網段
  * 192.83.177.0/24、192.83.178.0/24
  * 上述可否使用 192.83.177.0/23 表示??

192.83.177.0/23 是否有誤?

- 設定 Static Route
  - (config)# ip route 192.83.177.0 255.255.254.0 192.192.7.234
  - 錯誤: "%Inconsistent address and mask"
- 正確 Static Route
  - # ip route 192.83.176.0 255.255.254.0 192.192.7.234
  - # ip route 192.83.178.0 255.255.254.0 192.192.7.234
- 原因
  - 192.83.177.0/23 非正確網段表示
  - /23 僅允許網段第三段為偶數。

結論

- 非任意連續兩筆 /24 皆可合併成 /23
- 中央氣象局 Static Route 需使用兩筆 /24
  - # ip route 192.83.177.0 255.255.255.0 192.192.7.234
  - # ip route 192.83.178.0 255.255.255.0 192.192.7.234
- Root Cause: 最初 IP 子網段分配不適當
  - 較佳之兩筆 /24 子網段分配
  - Case1: 192.83.176.0/23
    - 192.83.176.0/24、192.83.177.0/24(中央氣象局)
  - Case2: 192.83.178.0/23
    - 192.83.178.0/24(中央氣象局)、192.83.179.0/24

北醫雙和新校區

如何切網段

北醫雙和新校區

- 需求: 由現有網段切出四個 Class C 網段給新校區使用
- 北醫現有網段:
  - 203.64.48.0/22 (203.64.48.0~203.64.51.255)
  - 203.71.84.0/22 (203.71.84.0~203.87.255)
  - 203.71.88.0/21 (203.71.88.0~203.71.95.255)
  - 120.97.32.0/19 (120.97.32.0~120.97.63.255)
  - 120.97.64.0/20 (120.97.64.0~120.97.79.255)
- 該如何選擇切出最佳網段?

如何選擇四個 Class C 網段

- 北醫回覆由 120.97.32.0/19 切出四個網段
  - 120.97.34.0/24
  - 120.97.35.0/24
  - 120.97.36.0/24
  - 120.97.37.0/24
  - 原因(推測): 選擇最大網段切成小網段
- 缺點1: 四個網段無法由一筆路由表示
  - 120.97.34.0/22 非正常網段表示方式
    - (config)# ip route 120.97.34.0 255.255.252.0 10.0.0.1
    - %Inconsistent address and mask
    - 非任意連續四筆 /24 皆可合併成 /22 (需為 4的倍數)
  - 需使用兩筆網段表示
    - 120.97.34.0/23
    - 120.97.36.0/23

如何選擇四個 Class C 網段

* 缺點2: 網段碎片化
  * 原網段: 120.97.32.0/19，切割後需用六個網段表示
    * 120.97.32.0/23
    * 120.97.34.0/23 北醫雙和校區
    * 120.97.36.0/23 北醫雙和校區
    * 120.97.38.0/23
    * 120.97.40.0/21
    * 120.97.48.0/20
  * 區網端 Static Route 由 1 筆變成 6 筆
  * 影響 EBGP 放給區網與 ISP Peering 路由

如何選擇四個 Class C 網段較佳解法

* 四個 Class C 網段，等同 /22
* 優先使用目前 /22 網段
  * 203.64.48.0/22
  * 203.71.84.0/22
* 應先考慮由較小的網段來切
* 不要從中間切, 應從最前或最後來切網段

如何選擇四個 Class C 網段較佳解法

* 最後決定使用此網段切出四個 Class C
  * 120.97.64.0/20 (120.97.64.0 ~ 120.97.79.255)
* 切成三個子網段:
  * 120.97.64.0/22 (120.97.64.0 ~ 120.97.67.255) --> 雙和校區(4 Class C)
  * 120.97.68.0/22 (120.97.68.0 ~ 120.97.71.255)
  * 120.97.72.0/21 (120.97.72.0 ~ 120.97.79.255)

112年度區網課程(16門)

分類	日期	講題	講者	報名
大數據	7/19	Splunk:大型企業門禁系統安全事件日誌(實做課程)	黃國泰(阿甘)	27
大數據	7/25	Influxdb + Grafana - 時間序列數據視覺化的當紅炸子雞	Zoe 林宜欣	71
大數據	7/26	Splunk:作業系統安全事件日誌(實做課程)	黃國泰(阿甘)	30
大數據	8/2	Redis - 專案開發最百搭的暫存資料庫	Winston 盧文松	85
雲端	8/4	Google Workspace 超實用技巧 與 Google Classroom 實際應用場景	CloudMile 陳宏傑	65
網路	8/9	透過單一簽入解決方案整合地端應用系統與雲端服務認證	鉉迪資訊 鍾迪 資深技術顧問	89
雲端	8/11	人人皆開發：AppSheet 無程式碼開發教學（上）	CloudMile 陳宏傑	76
網路	8/15	ChatGPT應用於網路安全	劉得民老師	161

(線上12門 + 實做4門) 每堂課平均 68人

112年度區網課程(16門)

分類	日期	講題	講者	報名
雲端	8/18	人人皆開發：AppSheet 無程式碼開發教學（下）	CloudMile 陳宏傑	60
法規	8/23	資訊安全管理制度國際標準(ISO 27001:2022)簡介	資誠聯合會計師 Michael 黃承漢	101
雲端	8/24	Kubernetes 101 如何降低作業系統的限制-輕量化服務的世界(實做課程)	峰儀 曾光毅 資深技術顧問	41
雲端	8/25	提升報表力！ 資料視覺化，一用 Looker Studio 就上手	CloudMile 胡宇謙	63
法規	8/29	著作權合理使用之實務運作	胡中瑋 律師	53
雲端	8/31	Kubernetes with tools 如何有效管理輕量化服務系統(實做課程)	峰儀 曾光毅 資深技術顧問	38
雲端	9/8	無痛連結 Google Workspace, REST APIs（初階）	CloudMile 張家瑋	72
雲端	9/15	無痛連結 Google Workspace, REST APIs（進階）	CloudMile 張家瑋	54

(線上12門 + 實做4門) 每堂課平均 68人

連線單位互動

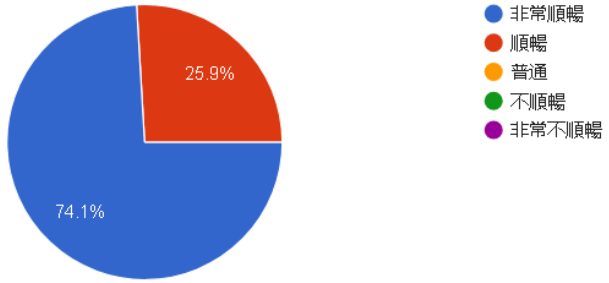
* 區網網管會議
  * 112年第一次網管會議出席率:74%
    * 因開會時間於暑假開始之第一週，許多網管老師已安排活動，未來將避免於暑假期間舉行。

* 連線單位滿意度調查
  * **53連線單位，收到54份回覆**
  * **回覆率100%**

滿意度調查結果 part1

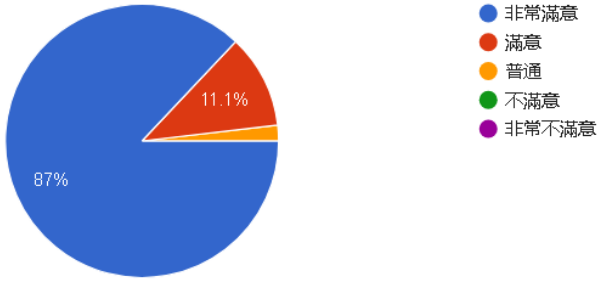
本年度　貴單位之網路連線服務，順暢與否?

54 則回應



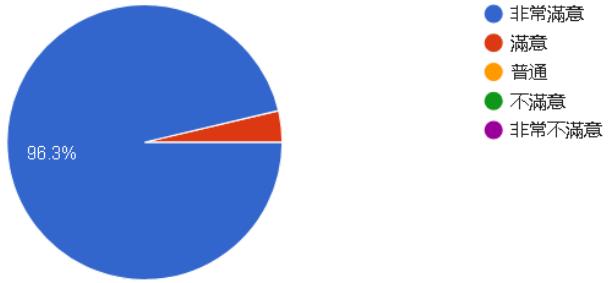
資通安全事件的通報應變的協助處理:

54 則回應



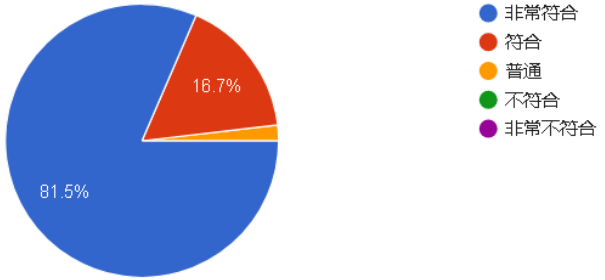
本年度　貴單位如有網路管理或連線問題時，區網中心的協助是否有順利排除障礙?

54 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?

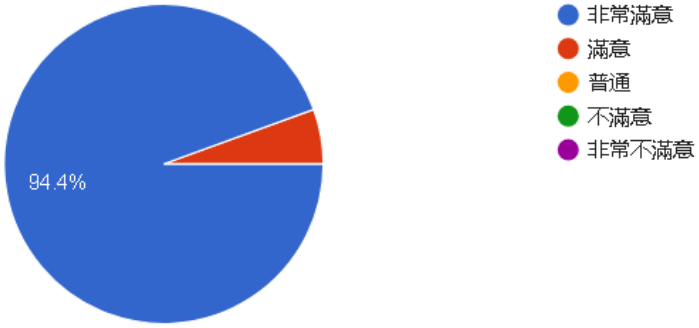
54 則回應



滿意度調查結果 part2

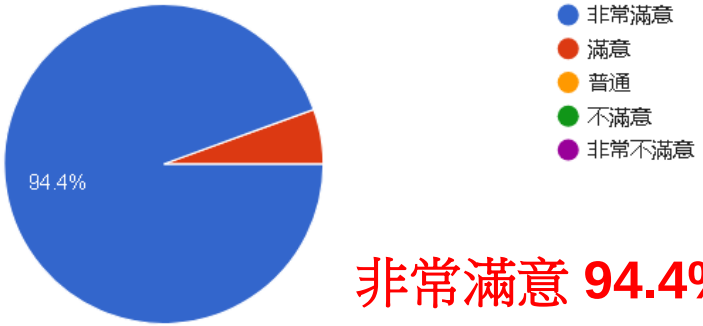
貴單位對於區網中心服務人員之熱忱及親和力的滿意度?

54 則回應



貴單位對於區網中心綜合整體服務的表現

54 則回應



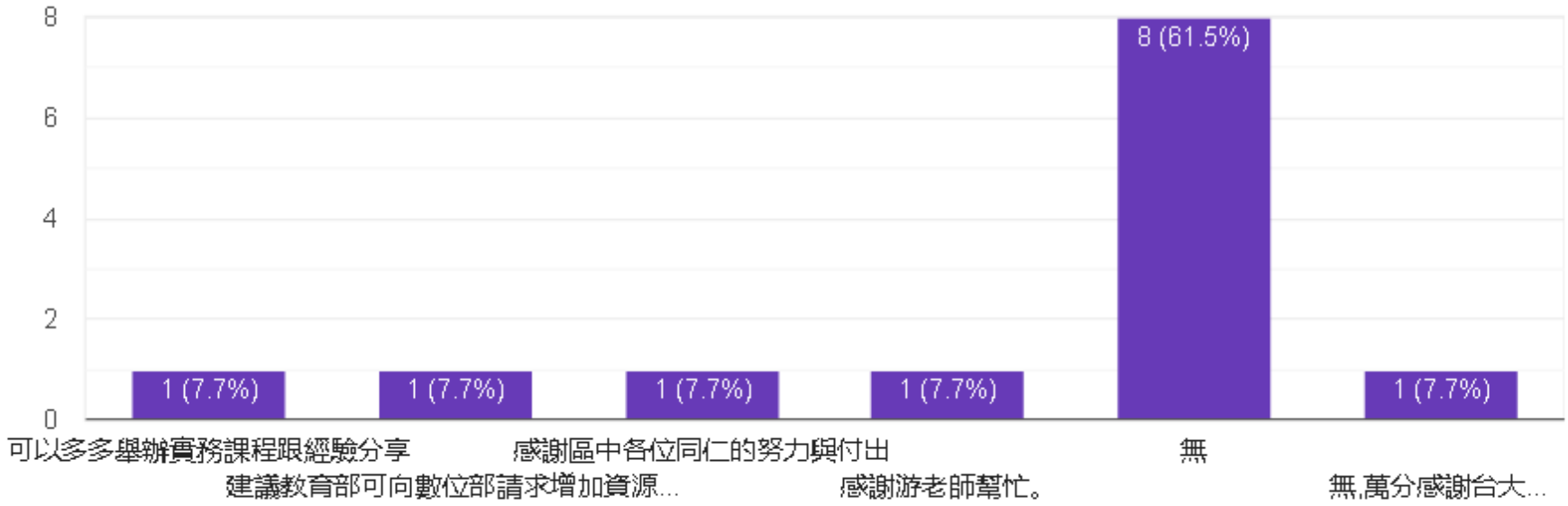
非常滿意 94.4%

滿意度調查結果 part3

對區域網路中心在網路維運管理的建議

複製

13 則回應



滿意度調查結果 part4

對區網所舉辦之教育訓練或研習課程建議

13 則回應

希望能繼續保有線上課程

希望多開一些資通安全職能訓練課程，私校也可參與

無。

未來機房與骨幹建設的規劃

希望開Wireshark課程

希望能多開設基礎資安技術檢測或資安攻防等實體上機操作課程，謝謝。

希望能提供線上參與

希望游子興老師能多舉辦區網會議，講解準備的投影片內容，每次會議聽老師講課，對於網管方面的知識都很有收穫。

可以多多舉辦實務課程跟經驗分享

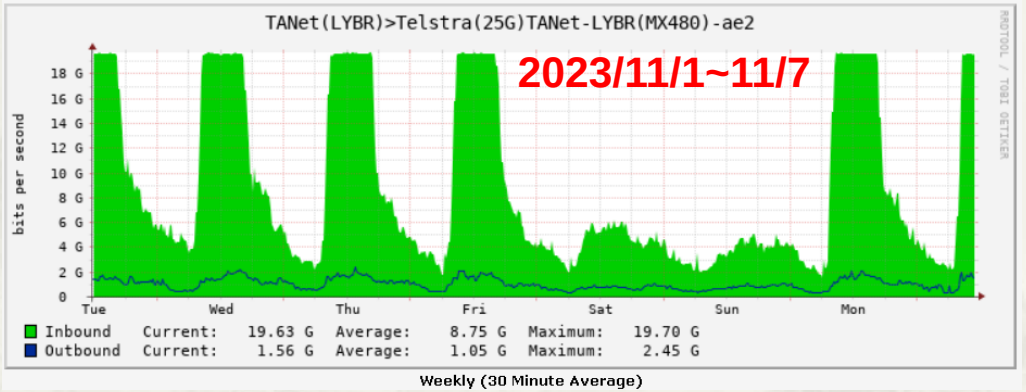
8.1 未來營運目標

* 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
* 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

評審委員: 網路妥善率 **99.9%**，建議明確目標延伸至小數點下 **2** 位數。

8.2 其他建議

* 儘速解決國際頻寬 Telstra 壅塞問題
  * 使用者: 網站 login.imedidata.com 於美東AWS. 常出現 time out 白畫面.



* 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