113年度第一次
台北區網(臺大)網管會議

臺灣大學計資中心
游子興
davisyou@ntu.edu.tw
3366-5008

會議議程

項目	時 間	報告人	報 告 內 容
主席報告	14:00~14:05	謝宏昀教授	
業務報告	14:05~14:20	游子興	區網營運業務報告
	14:20~14:30	史詩妤	資安事件相關說明
	14:30~14:50	李美雯	資安 Case Study分享
專題演講	15:00~16:00	台大醫院-胡勝倫	從 syslog 到網路聯防機制
	16:00~17:00	游子興	1.ProxyARP 原理與案例分享 2.Proxmox Virtual Environment (PVE) 開源伺服器虛擬化環境
臨時動議		出列席人員	

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

https://tools.ipip.net/traceroute.php

IPv4 | 新加坡(GCP) | ICMP | 163.28.16.254 | 查看

台大區網 IP

目标 IP：163.28.16.254

跳数	IP	主机名	地区（仅供参考）	AS号（仅供参考）	时间（毫秒）
1	*	*	*	*	*
2	*	*	*	*	*
3	202.84.249.161	i-15650.hkck-core01.telstraglobal.net	中国香港 telstra.com	AS4637	31.8 / 33 / 33
4	*	*	*	*	*
5	202.84.230.90	202.84.230.90	中国台湾台北市 telstra.com	AS4637	45.3 / 47 / 94
6	210.176.44.178	unknown.telstraglobal.net	中国台湾台北市 telstra.com	AS4637	44.9 / 45.1 / 283
7	192.192.68.63	192.192.68.63	中国台湾台北市 edu.tw	AS1659	251.4 / 503.9 / 507.9
8	192.192.61.59	192.192.61.59	中国台湾台北市 edu.tw	AS1659	235.9 / 236.2 / 254
9	192.192.61.49	192.192.61.49	中国台湾台北市 edu.tw	AS1659	212.1 / 222 / 239.5
10	163.28.16.254	gateway163-16.ntu.edu.tw	中国台湾台北市 edu.tw	AS17716 / AS1659	47.4 / 210 / 491

IPv4 | 新加坡(GCP) | ICMP | 163.14.1.1

東吳大學 IP

目标 IP：163.14.1.1

跳数	IP	主机名	地区（仅供参考）	AS号（仅供参考）	时间（毫秒）
1	*	*	*	*	*
2	72.14.196.230	72.14.196.230	中国台湾台北市 google.com	AS15169	180.5 / 180.7 / 181.9
3	*	*	*	*	*
4	*	*	*	*	*
5	*	*	*	*	*
6	*	*	*	*	*

GCP(Google Cloud Platform) 無法連線

- 2024/06 教育部區縣市網期中會議提出
  - 教育部回覆: 先前已與中研院、Google 開會協調，但仍無法解決，需等明年新的學網400G骨幹建設完成後, 與 Google 建立 Peering 電路後才能解決.
- 暫時解法:
  - 將目的 IP: 35.208.0.0 255.240.0.0 使用非學網 IP 連線 (將學網 IP 經 NAT 轉成 ISP IP 連線)
    - 政大提供方法

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

區網會議主題分享

- 每學期區網會議
- 時間: 1 HR (講師費 $2000)
- 可分享主題
  - 網路、機房基礎建設、跨校區網路規劃
  - 資安防護
- 已經分享
  - 國立臺灣大學醫學院附設醫院
  - 國立臺灣師範大學(公館校區)
  - 國立臺北藝術大學
  - 臺北醫學大學
  - 台北海洋科技大學
  - 臺北科技大學

區網會議主題分享

- 國防大學（復興崗校區）
- 國防醫學院
- 國立空中大學
- 國立臺北護理健康大學
- 國立臺灣藝術大學
- 國立臺北商業大學
- 銘傳大學
- 實踐大學
- 真理大學
- 大同大學
- 龍華科技大學
- 宏國德霖科技大學
- 亞東科技大學
- 致理科技大學
- 黎明技術學院
- 康寧大學
- 華夏科技大學
- 私立明志科技大學
- 德明財經科技大學
- 法鼓文理學院
- 臺北市立大學
- 臺北基督學院
- 臺灣科技大學
- 東吳大學

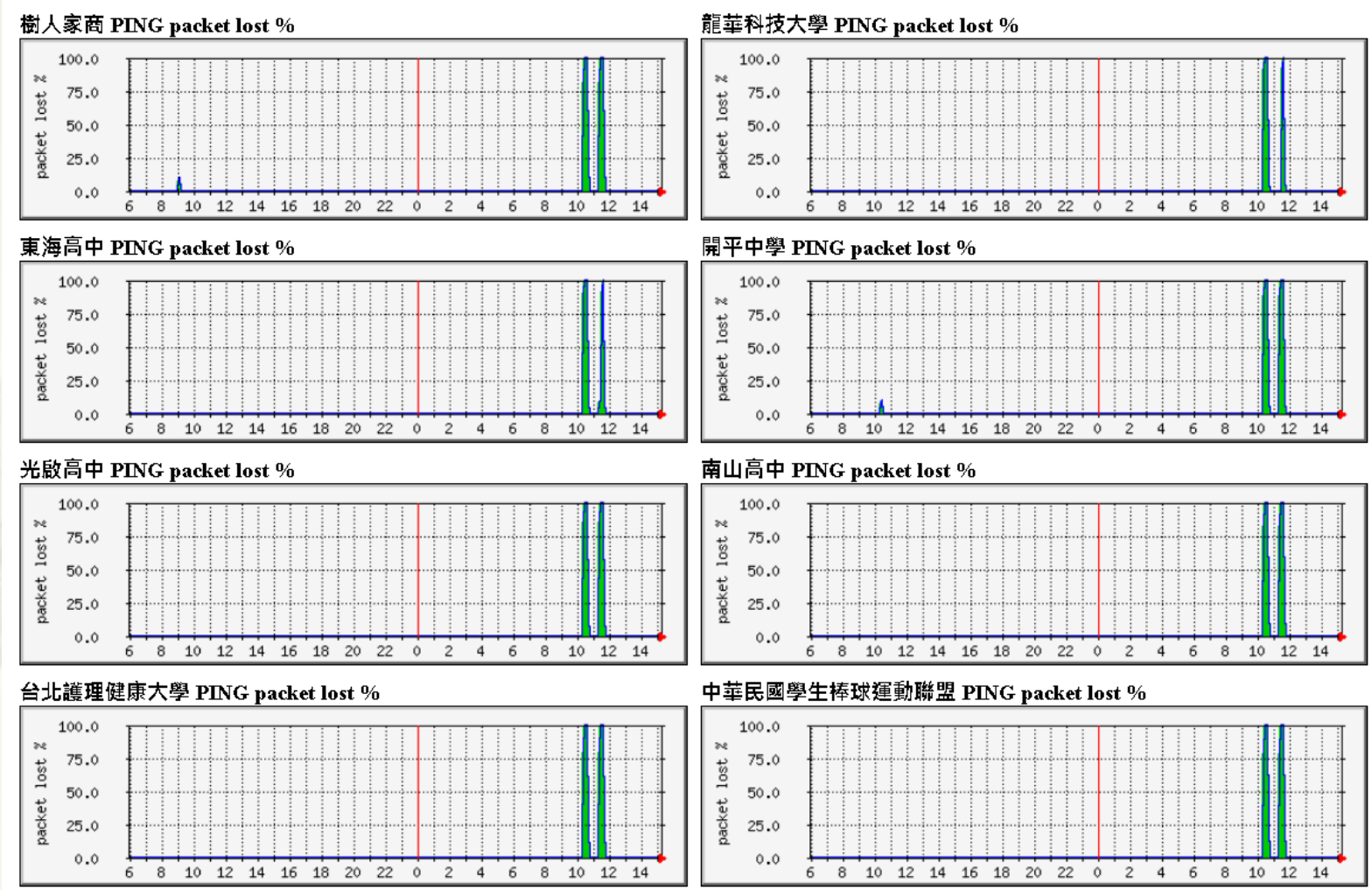
區網暑期課程

分類	課程	教室	講題	講者
資安	7/16 14:00~17:00	R106	駭客攻擊手法深入探討	中華資安 林峰正
雲端	7/19 15:00~17:00	線上	檔案不再雜亂無章：使用 Google Workspace 打造超流暢工作流	CloudMile 陳宏傑
系統	7/24 9:30~12:00 13:00~16:30	R212	Proxmox VE 虛擬環境實做上機課程	南投縣網 鄭明彰、節省哥
雲端	7/26 15:00~17:00	線上	Google Classroom 實際應用場景	CloudMile 陳宏傑
雲端	8/2 15:00~17:00	線上	解鎖工作效率新境界：Gemini for GWS 實戰應用	CloudMile 鄭潯元
法規	8/6 15:00~17:00	R106	AI 著作權議題	胡中瑋律師
雲端	8/9 15:00~17:00	線上	透過 AppScript Generative AI (Gemini API) 整理 Gmail 信件內容	CloudMile 張家瑋
大數據	8/13 14:00 ~ 17:00	R106	ML, AI 於 ELK 上的應用	集先鋒 Anthony 陳俊佑
資安	8/15 15:00~17:00	R106	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
雲端	8/16 15:00~17:00	線上	無痛連結 Google Workspace, REST APIs（初階）	CloudMile 陳智聰
雲端	8/23 15:00~17:00	線上	無痛連結 Google Workspace, REST APIs（進階）	CloudMile 陳智聰
AI	8/29 15:00~17:00	R106	以Pure Storage 平台來加速擁抱 AI 的驅動力	Pure Storage 蔣燚峰
資安	8/30 14:00~17:00	R212	網站常見弱點檢測與修補(老師期待電腦教室有實作)	凱老師
網路	9/4 14:00~17:00	R106	網路設備常見規格及網路異常排除方法	子興、詩妤
資安	9/6 14:00-17:00		常見的網站漏洞利用以及防禦介紹	中華資安 蕭子修
資安	9/9 14:00~17:00	R212	滲透測試LAB實作練習 (有LAB)	中華資安 蔡侑達

歡迎加入區網 **Line** 群組

ASR9K 韌體升級
2024/02/18

ASR9K 韌體升級斷線過程



ASR9K 韌體升級斷線過程

* 斷線時間共兩次
  * 10:26 ~ 10:37 (11分鐘)
  * 11:27 ~ 11:39 (12分鐘)
* PingInfo View 監控 168.95.1.1 斷線記錄

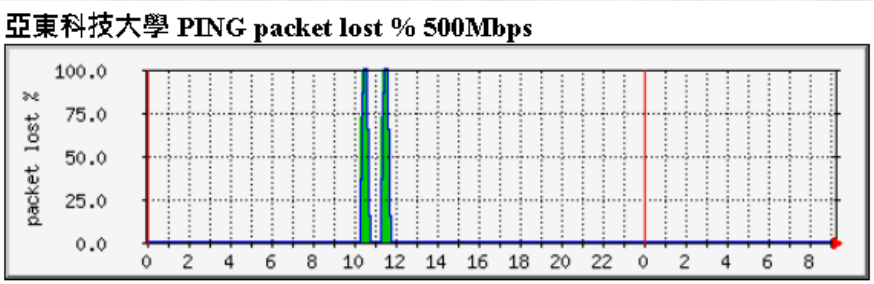
Order	Host Name	IP Address	Description
4	168.95.1.1	168.95.1.1	DNS

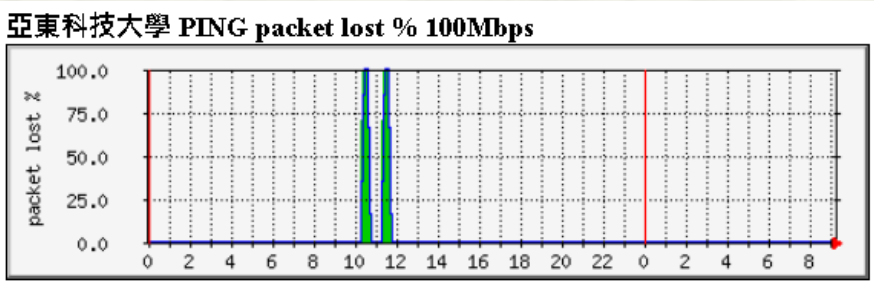
Sent On	Reply IP Ad
2024/2/18 上午 11:40:45 - 2024/2/18 下午 03:34:35	168.95.1.1
2024/2/18 上午 11:27:32 - 2024/2/18 上午 11:39:44	
2024/2/18 上午 10:38:44 - 2024/2/18 上午 11:26:31	168.95.1.1
2024/2/18 上午 10:26:32 - 2024/2/18 上午 10:37:43	
2024/2/16 下午 12:09:59 - 2024/2/18 上午 10:25:31	168.95.1.1

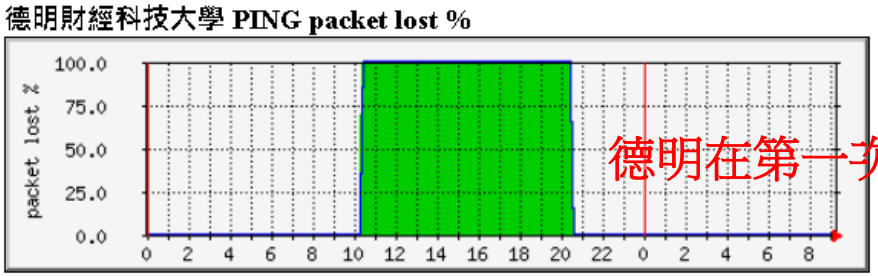
德明財經科技大學
ASR9K 韌體升級後斷線
問題釐清與記錄

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)
* 封包遺失 MRTG



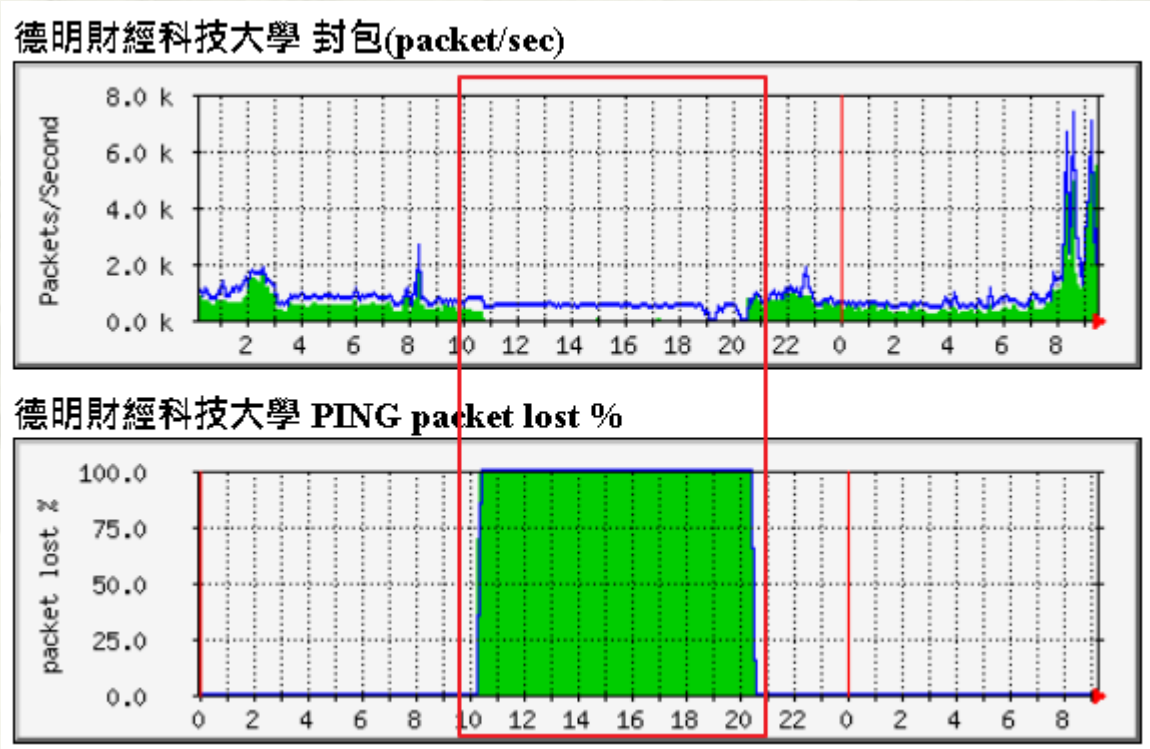




德明在第一次斷線後就沒有恢復

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



台大區網 ASR
德明科大介面流量

- Input: 流量很少，但有收到 → 德明 to 台大 電路正常
- Output: 4Mbps →台大端 路由設定與 SFP 正常

```
RP/0/RP0/CPU0:TANet-NTU-ASR9912-01#sh int GigabitEthernet0/7/0/8
Sun Feb 18 20:05:50.832 CST
GigabitEthernet0/7/0/8 is up, line protocol is up
  Interface state transitions: 15
  Hardware is GigabitEthernet, address is 046c.9d55.6328 (bia 046c.9d55.6328)
  Internet address is 192.192.7.57/30
  MTU 1514 bytes, BW 1000000 Kbit (Max: 1000000 Kbit)
     reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation ARPA,
  Full-duplex, 1000Mb/s, LXFDX, link type is force-up
  output flow control is off, input flow control is off
  Carrier delay (up) is 10 msec
  loopback not set,
  Last link flapped 00:00:06
  ARP type ARPA, ARP timeout 04:00:00
  Last input 00:00:00, output 00:00:00
  Last clearing of "show interface" counters never
  30 second input rate 5000 bits/sec, 3 packets/sec
  30 second output rate 39000 bits/sec, 64 packets/sec
```

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

德明科大介面封包側錄 @區網端

- Ping 德明科大介面 IP 192.192.7.58
- 無回應，封包側錄有看到 ICMP Ping 封包

```
RP/0/RP0/CPU0:TANet-NTU-ASR9912-01#ping 192.192.7.58
Sun Feb 18 19:46:24.477 CST
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.192.7.58, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

icmp and ip.addr==192.192.7.57

).	Vlan	Source	Destination	Src MAC	Dst MAC	Protocol	Length	Info
449		192.192.7.57	192.192.7.58	Cisco_55:63:22	Fortinet_09:00:11	ICMP	114	Echo (ping) request
1309		192.192.7.57	192.192.7.58	Cisco_55:63:22	Fortinet_09:00:11	ICMP	114	Echo (ping) request
2480		192.192.7.57	192.192.7.58	Cisco_55:63:22	Fortinet_09:00:11	ICMP	114	Echo (ping) request
3373		192.192.7.57	192.192.7.58	Cisco_55:63:22	Fortinet_09:00:11	ICMP	114	Echo (ping) request

@德明科大
使用 **ASUS** 筆電 直連

* 台大端有學到 ARP → 德明 to 台大 電路正常

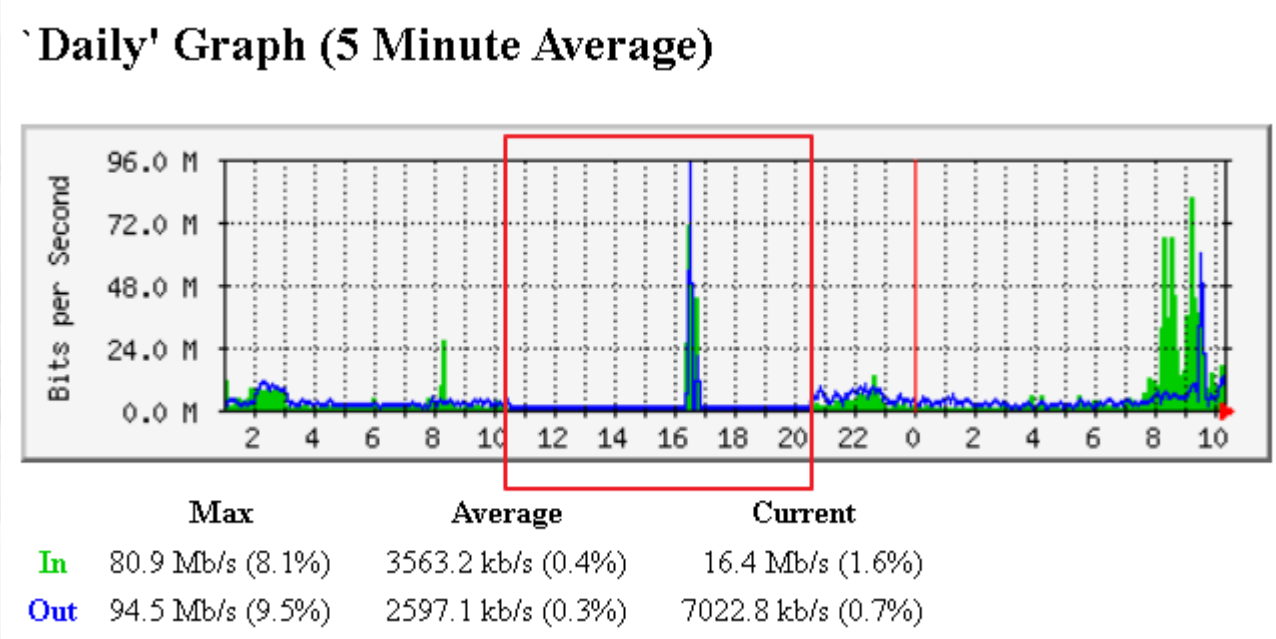
```
sh arp GigabitEthernet0/7/0/8
Sun Feb 18 19:35:12.819 CST
------------------------------------------------------------------------------
0/7/CPU0
------------------------------------------------------------------------------
Address         Age        Hardware Addr   State      Type  Interface
192.192.7.57    -          046c.9d55.6328  Interface  ARPA  GigabitEthernet0/7/0/8
192.192.7.58    00:00:00   0442.1a00.6547  Dynamic    ARPA  GigabitEthernet0/7/0/8
```

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

德明科大端介面 MRTG

* 斷線期間無收到台大端流量
  * 16:00 ~ 17:00 為何有流量? (原因不明)



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

簡報完畢
謝謝