南投區域網路中心
期末審查

報告人：俞旭昇主任

大綱

一.區網基礎維運

(一)經費及人力

1.網路中心經費使用

2.網路中心人力

(二)網管及資安

1.網路中心連線情形

2.資訊安全環境整備

(三)策略及具體辦理事項

(四)資安管理與服務

(五)網管及資安人力績效

二、區網服務特色

(一)工作成效

(二)未來目標

區網基礎維運

經費及人力-經費使用

核定計畫金額：1,449,866

教育部補助金額：1,449,866

實際累計執行數（至11/15）：85% (兩位計畫助理薪資及年終獎金)

自籌金額：1,785,600

- ✓ 中心電腦主機房UPS不斷電系統汰換1,785,600

區網基礎維運

經費及人力-網路中心人力數

專任：20人　　兼任：1人

其中包含教育部補助

網管人員：1人，證照數：2 張

（ISO 27001 資訊安全管理系統、BS 10012個人資料管理系統）

資安人員：1人，證照數：4張。

(ITE 網際網路介接基礎、ITE 資料通訊、ITE 網際網路服務與應用、ITE 網路安全）

區網基礎維運

網管及資安-連線情形

項目(校數)		大專	高中職	其他	總計	
（1）區網中心連線學校數:		1	9	9	19	19（不含縣網中心）
區網中心連線學校連線方式	ADSL（校）					
	專線（校）	1			1	暨南大學
	光纖10M（校）					
	光纖100M（校）		9	8	17	**高中職：** 水里商工、普台高中、南投高中、仁愛高農、三育高中、五育高中、同德家商、埔里高工、暨大附中 **其他：** 均頭國中，台大實驗林清水溝分部、溪頭分部水里分部、水里木材實驗工廠分部、下坪分部內茅埔分部、和社分部
	其他20M			1	1	台大實驗林竹山本部
連線縣(市)網路中心：		南投縣網中心				

本年度協助暨大附中及埔里高工由10M升級至100M

區網基礎維運

網路中心及連線學校資安事件緊急通報處理之效率及通報率

	104年度	105年度
1、2級資安事件	(1)自行通報數：7件。 (2)非自行通報數：344件。 (3)通報平均時數：0.46小時。	(1)自行通報數：5件。 (2)非自行通報數：205件。 (3)通報平均時數：0.29小時。
	無3、4級資安事件	
平均時數	平均審核時數：0.26小時。	事件平均處理時數:0.29小時。 平均審核時數：0.17小時。 資通安全通報應變平台之聯絡相關資訊完整度：92.31%

通報完成率及事件完成率皆為100%

區網基礎維運

網路中心配合本部資安政策。

2. 區網網路中心依資通安全應執行事項::

(1)是否符合防護縱深要求? ■是 □否

(2)是否符合稽核要求? ■是 □否

(3)符合資安專業證照人數：7員

本中心陳順德組長、黃景煌資料管理師、楊文龍技術員、楊世偉技術員、何奇芳技術員、黃仁宏技術員、劉育瑄專任助理皆考取ISMS主導稽核員證照

陳彥良專任助理考取ITE 網際網路介接基礎、ITE 資料通訊、ITE 網際網路服務與應用、ITE 網路安全

(4)維護之主要網站進行安全弱點檢測比率：100%。

區網基礎維運

單位策略及具體完成事項

節電及綠能降低PUE值：

機房加裝自然進氣系統，節省機房電費，UPS 110V改220v提高電力轉換效率

- ✓ 原機房內共有三台UPS
  Input 380/220v Output 190/110v，轉換效率90%
- ✓ 建置模組化UPS一台，其容量可透過模組的擴充增加
  Input 380/220v Output 380/220v，轉換效率96%

資源共享：

提供VM主機供連線單位申請使用、提供縣網境內國中小網頁空間

區網基礎維運

單位策略及具體完成事項

網路品質的維持：

導入What's UP網管軟體、繪製流量圖供下游單位查詢

資安事件：

協助查修事件類型及分析，讓連線單位資訊教師能迅速排除問題

協助教育部相關計畫：

協助遠距課輔硬體及網路維護，及維持課輔品質

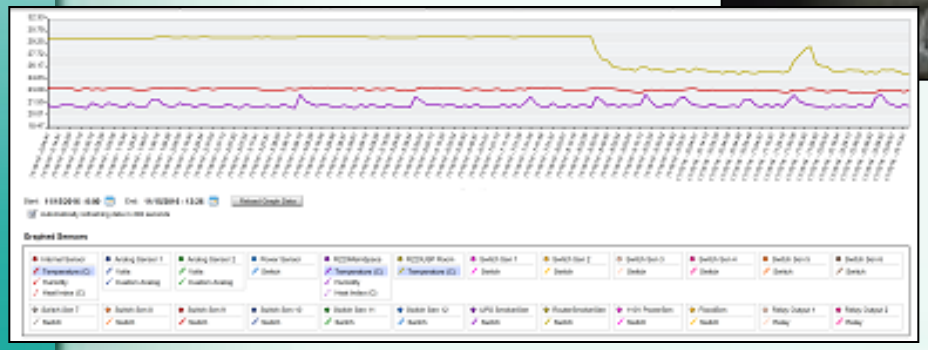
區網基礎維運

單位策略及具體完成事項

實體環境：

安裝整合式環境監測系統、並與成功大學異地備份/備援

- ✓ 電力
- ✓ 漏液
- ✓ 偵煙
- ✓ 溫濕度

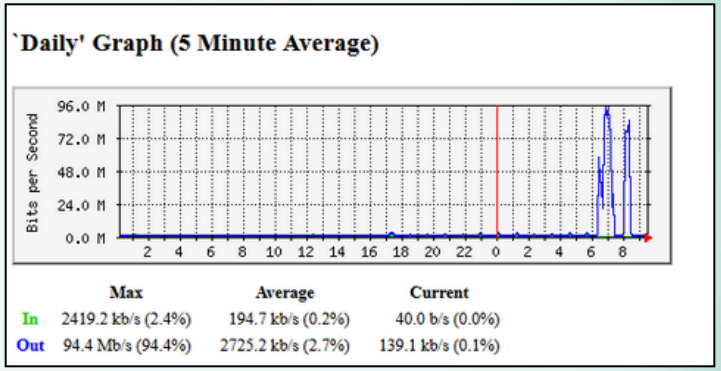


溫度系統計錄表

區網基礎維運

資安管理與服務辦理事項

- 協助連線單位資安通報查修，有效降低資安通報量
- 如連線單位網路斷線，由系統主動E-mail通知連線單位聯絡人
- 協助連線單位阻檔DDoS攻擊
  - ✓ 國立仁愛高農
  - ✓ 均頭國中
  - ✓ 南投縣仁愛鄉合作國民小學
  - ✓ 國立南投高級商業職業學校



DDoS攻擊時的流量圖

Top Destinations

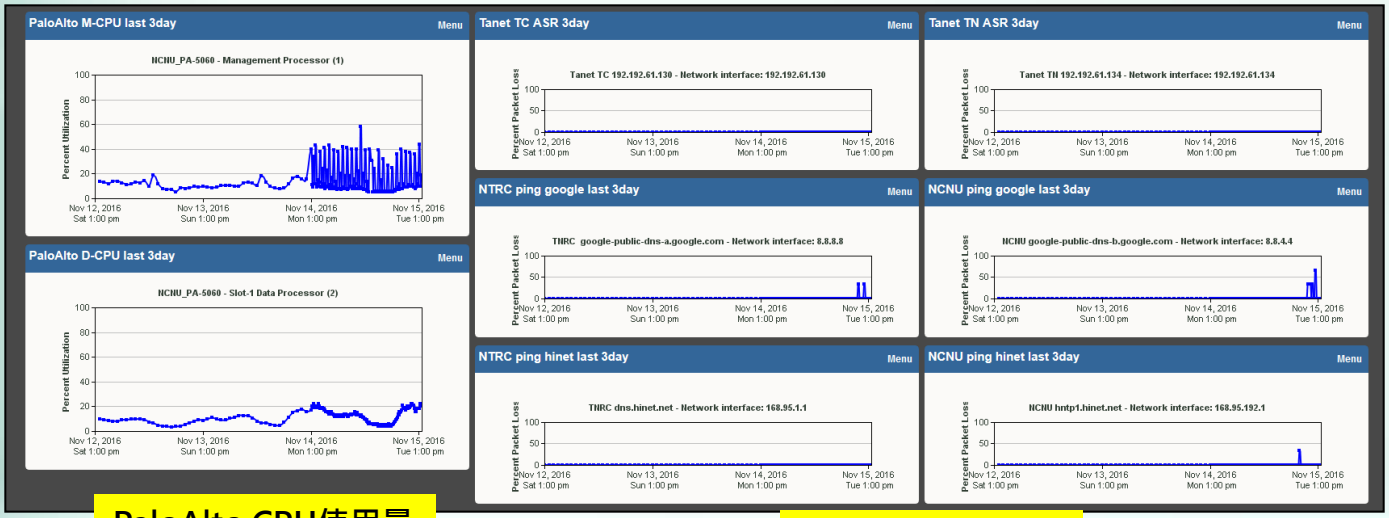
	Destination Address	Destination Host Name	Destination User	Bytes	Sessions
1	163.22.160.102	web.ravs.ntct.edu.tw		74.6 G	23.7 M
2	168.95.1.1	dns.hinet.net		483.3 M	2.1 M
3	8.8.8.8	google-public-dns-a.google.com		184.9 M	779.8 K
4	211.79.61.47	dns3.twaren.net		113.3 M	523.1 K
5	168.95.192.1	hntp1.hinet.net		117.1 M	487.2 K

PaloAlto顯示資訊

區網基礎維運

網管及資安人力之服務績效

1. 資安通報之通報、應變、審核及資安事件資料收集及分析
2. 推動ISMS資訊管理系統
3. 舉辦資安或開源軟體研討會
4. 舉辦連線單位管理委員會
5. 骨幹網路監測及故障排除



PaloAlto CPU使用量

骨幹網路監測圖

區網基礎維運

網管及資安人力之服務績效

6. 機房環境監測及電力設備維護
7. 提供連線單位技術協助及各事項反應及聯絡窗口
8. 計畫經費控管及承接計畫相關行政流程
9. 配合教育部進行資安通報演練及業務持續作業演練計畫
10. 其他教育部臨時交辦事項
11. 配合教育部100G安裝測試線路轉移
12. 協助縣網P2P下載封鎖

Generate Time	Type	From Zone	To Zone	Source	Destination	From Port	To Port	IP Protocol	Application	Action	Rule	Bytes	Bytes Sent	Bytes Received
11/15 13:47:23	deny	100G_Tanet_In	100G_Tanet_Out		92.97.146.57	6881	1472	udp	bittorrent	deny	Tanet_p2p_block	147	147	0
11/15 13:47:23	deny	100G_Tanet_In	100G_Tanet_Out		188.222.180.230	6881	50321	udp	bittorrent	deny	Tanet_p2p_block	147	147	0
11/15 13:47:23	deny	100G_Tanet_In	100G_Tanet_Out		68.228.246.169	6881	29934	udp	bittorrent	deny	Tanet_p2p_block	147	147	0
11/15 13:47:18	deny	100G_Tanet_In	100G_Tanet_Out		188.24.101.251	6881	1024	udp	bittorrent	deny	Tanet_p2p_block	147	147	0
11/15 13:46:22	deny	100G_Tanet_In	100G_Tanet_Out		84.216.237.186	6881	50321	udp	bittorrent	deny	Tanet_p2p_block	147	147	0
11/15 13:46:22	deny	100G_Tanet_In	100G_Tanet_Out		98.250.248.176	6881	6889	udp	bittorrent	deny	Tanet_p2p_block	147	147	0
11/15 13:46:22	deny	100G_Tanet_In	100G_Tanet_Out		122.249.238.174	6881	6889	udp	bittorrent	deny	Tanet_p2p_block	147	147	0
11/15 13:46:21	deny	100G_Tanet_In	100G_Tanet_Out		118.151.208.40	6881	41563	udp	bittorrent	deny	Tanet_p2p_block	147	147	0
11/15 13:46:21	deny	100G_Tanet_In	100G_Tanet_Out		118.71.16.40	6881	3800	udp	bittorrent	deny	Tanet_p2p_block	147	147	0
11/15 13:46:21	deny	100G_Tanet_In	100G_Tanet_Out		92.224.17.186	6881	45577	udp	bittorrent	deny	Tanet_p2p_block	147	147	0
11/15 13:46:21	deny	100G_Tanet_In	100G_Tanet_Out		14.183.208.40	6881	3801	udp	bittorrent	deny	Tanet_p2p_block	147	147	0
11/15 13:46:11	deny	100G_Tanet_In	100G_Tanet_Out		175.133.55.159	6881	24368	udp	bittorrent	deny	Tanet_p2p_block	147	147	0
11/15 13:46:11	deny	100G_Tanet_In	100G_Tanet_Out		114.71.226.72	6881	50045	udp	bittorrent	deny	Tanet_p2p_block	147	147	0
11/15 13:46:11	deny	100G_Tanet_In	100G_Tanet_Out		66.87.114.21	6881	10026	udp	bittorrent	deny	Tanet_p2p_block	147	147	0
11/15 13:46:11	deny	100G_Tanet_In	100G_Tanet_Out		99.225.246.70	6881	50321	udp	bittorrent	deny	Tanet_p2p_block	147	147	0
11/15 13:46:11	deny	100G_Tanet_In	100G_Tanet_Out		36.226.140.165	6881	9361	udp	bittorrent	deny	Tanet_p2p_block	147	147	0
11/15 13:46:11	deny	100G_Tanet_In	100G_Tanet_Out		178.32.217.47	6881	6881	udp	bittorrent	deny	Tanet_p2p_block	147	147	0
11/15 13:46:11	deny	100G_Tanet_In	100G_Tanet_Out		158.181.30.162	6881	59363	udp	bittorrent	deny	Tanet_p2p_block	147	147	0
11/15 13:46:11	deny	100G_Tanet_In	100G_Tanet_Out		188.2.31.48	6881	58166	udp	bittorrent	deny	Tanet_p2p_block	147	147	0
11/15 13:46:11	deny	100G_Tanet_In	100G_Tanet_Out		192.187.100.162	6881	6882	udp	bittorrent	deny	Tanet_p2p_block	147	147	0

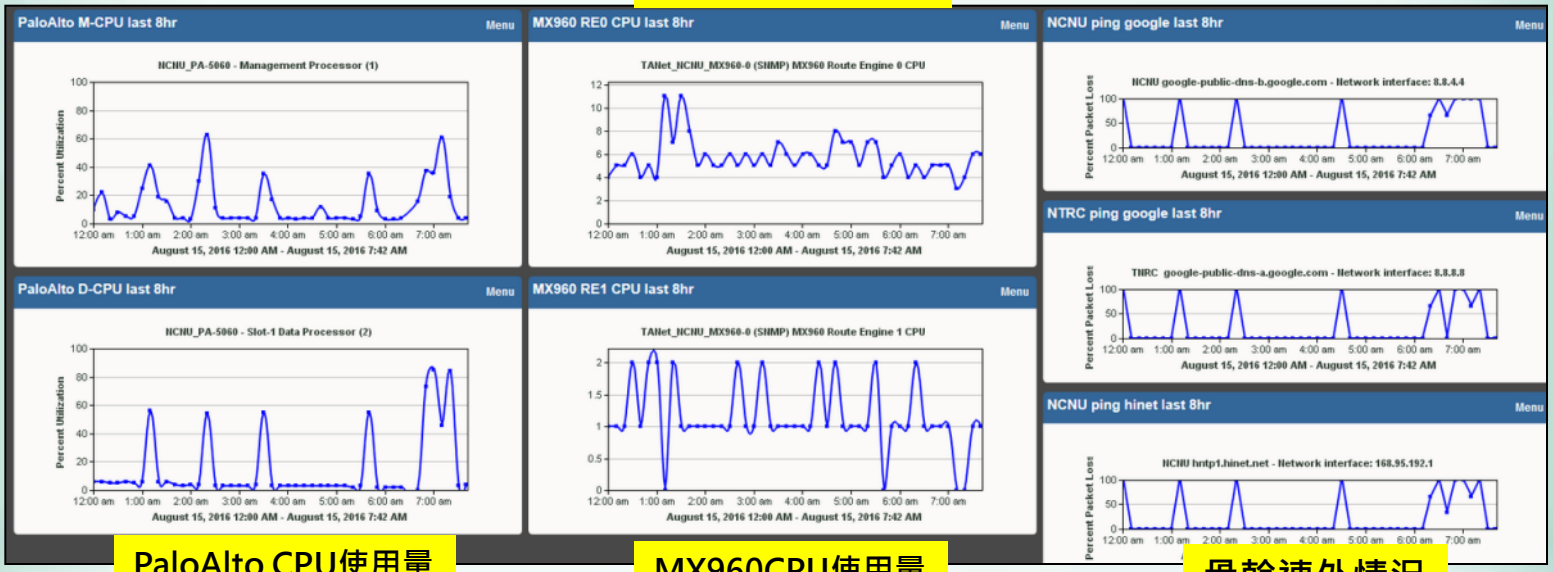
區網基礎維運

網管及資安人力之服務績效

13. 阻檔DDoS攻擊

- 8/15日區網遭受DDoS攻擊，連外網路不穩
- 先於PaloAlto上設定阻檔受害IP，PaloAlto CPU由80降到40

8/15日00:00~8:00



PaloAlto CPU使用量

MX960CPU使用量

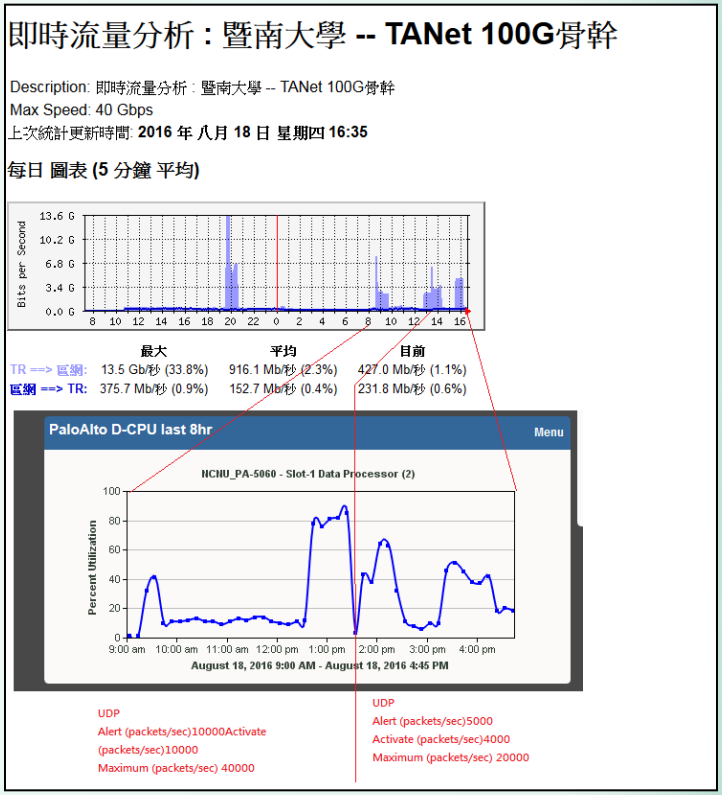
骨幹連外情況

區網基礎維運

網管及資安人力之服務績效

13. 阻檔DDoS攻擊

- 8/17日開始有大流量的攻擊產生，其目標並非單一IP，原先封鎖IP之規則不適用，攻擊流量>10G，設定Zone protection，流量降低至7G，連外網路恢復正常
- 8/18日早上無法連外，且PaloAlto管理介面也無法連線，先行by pass線路並設定DDoS Protection中UDP規則，上線後網路恢復正常

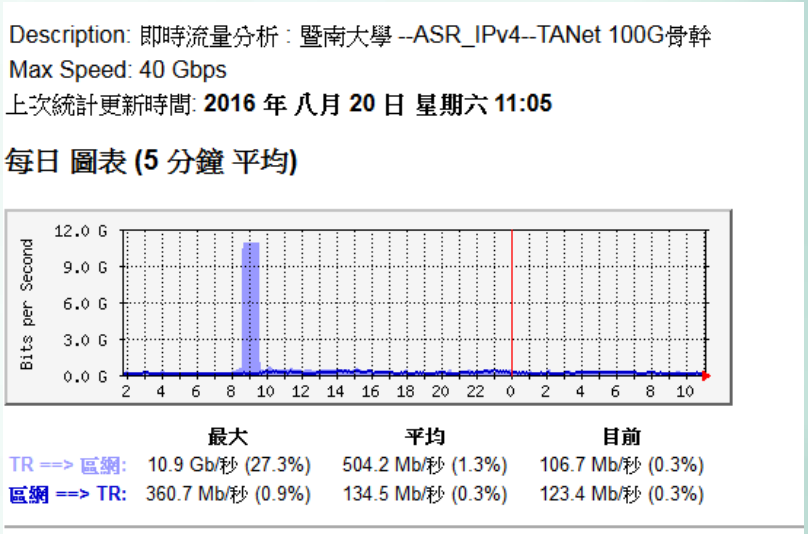


區網基礎維運

網管及資安人力之服務績效

13. 阻檔DDoS攻擊

- 8/18日中午過後又發生連外不穩的狀況，查詢後發現是PaloAlto CPU高達80%，再度by pass線路，下修DDoS Protection中UDP規則，上線後網路恢復正常



- 8/19日後就無大流量攻擊，但改成大量session數攻擊，其攻擊量最大紀錄到8,000,000 session數，遠超過PaloAlto最大承載量4,000,000 session數，造成PaloAlto管理介面自動重開多次，8/20日by pass線路後，連外網路恢復正常

區網基礎維運

網管及資安人力之服務績效

13. 阻檔DDoS攻擊

將線路by pass線路後，PaloAlto調整其規則並重新上線，調整規則如下

- ✓ 刪除Zone protection中所有規則
- ✓ 將多條DDoS Protection統整成一條規則
- ✓ 並加入最大Session數限制
- ✓ 上線後連外網路正常

PaloAlto重上線後，仍有DDoS攻擊狀況，但PaloAlto CPU使用率及連外網路正常，表示新設定規則達到預期效果，其統計資料如下

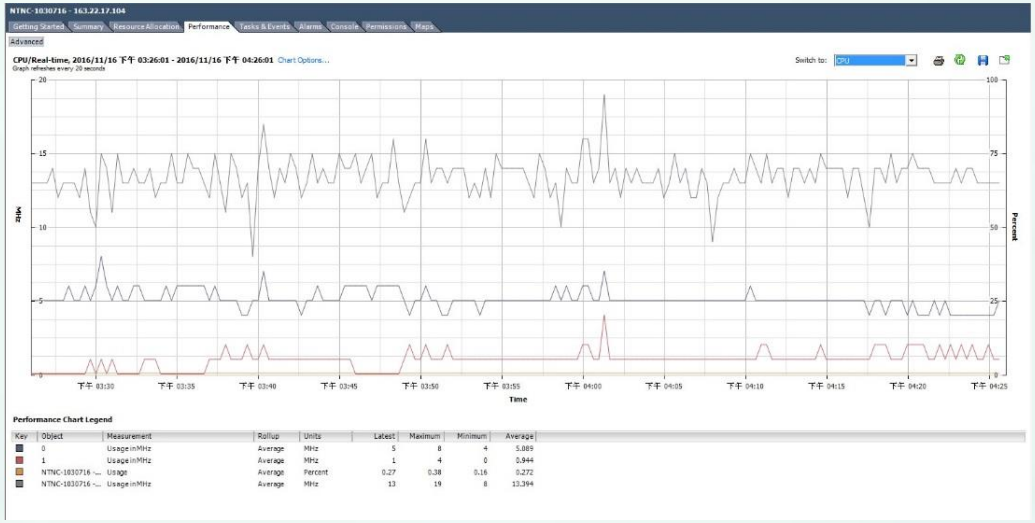
9/12 18:30 ~ 9/13 16:00

- ✓ UDP FLOOD 88,000,000
- ✓ Session Limit Event 3,300,000

區網中心服務特色

目前服務工作成效

1. 網路電話推廣：由區網架設SIP主機供連線單位使用
   2016年1月至11月通話時間 20523分 通數9481通
2. 提供縣網境內國中小網頁空間



區網中心服務特色

目前服務工作成效

3. 協助連線單位資安通報查修
   - ✓ 特徵是於http封包內user-agent欄位會寫BCWF Utilities，也就是Blue Coat Web Filter的縮寫
   - ✓ 於get的地方會填入一正常的網址http://www.youtube.com/443
   - ✓ 該校確定有安裝K9 Web Protection軟體
   - ✓ 並與Tacert通報做例外處理

區網中心服務特色

目前服務工作成效

4.管理委員會：

於10/13日舉辦管理委員會，並將於年終審查後12月份在舉辦一次管理委員會。

5.網路健檢：

暨大附中2次、埔里高工2次、台大實驗林4次

6.舉辦研討會：共舉辦兩場次

(1)10/21日課程內容為個資法令宣導講座、網路著作權與學術研究著作權、資訊安全及網路基本檢測

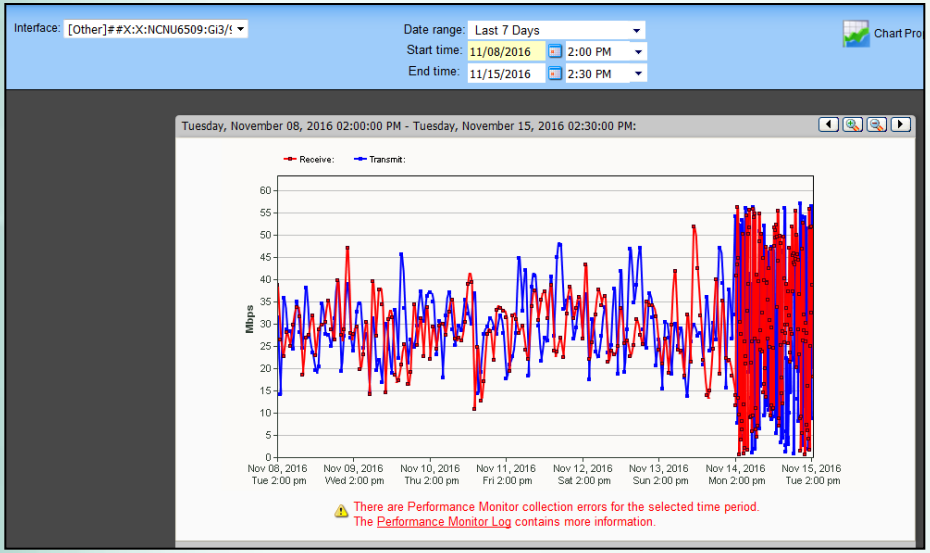
(2)10/26日課程內容為個資法令宣導講座、LibreOffice 辦公室應用

7.協助遠距課輔硬體及網路維護，維持課輔品質

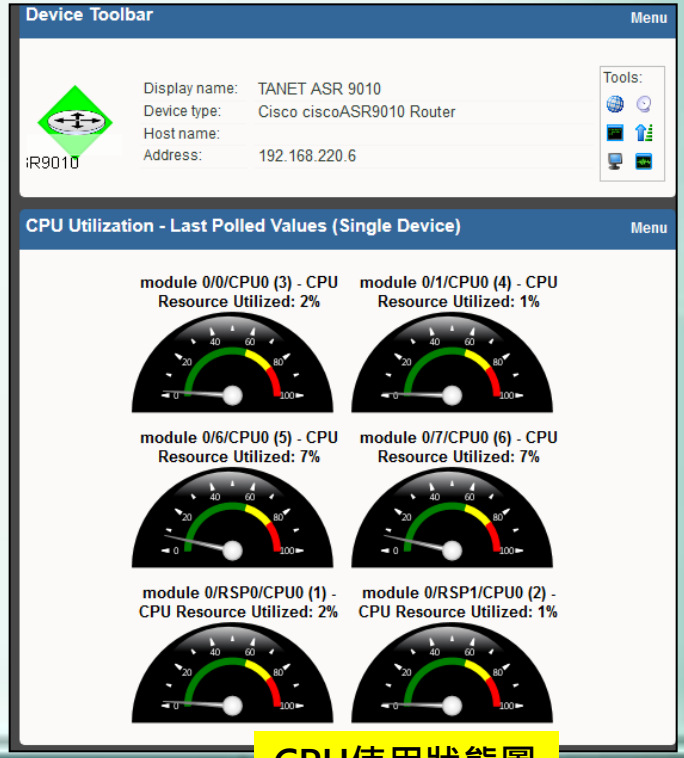
區網中心服務特色

目前服務工作成效

8. 將下游連線單位納入網管系統
9. 使用What’s UP繪製流量圖供下游單位查詢
10. 使用What’s UP監測連線單位設備



連線單位流量圖



CPU使用狀態圖

區網中心服務特色

目前服務工作成效

11. 如連線單位網路斷線，由系統主動E-mail通知連線單位聯絡人
12. 安裝整合式環境監測系統，加入漏液與偵煙
13. 協助台大實驗林竹山本部網路規劃
14. 導入ISMS資訊安全管理系統：已於本年度5月份完成第一次追查稽核

區網中心服務特色

未來服務工作目標

- ✓ 提供連線單位資安健檢
- ✓ 協助連線單位資安通報查修
- ✓ 提供多樣化的斷線通知機制
- ✓ 架設cacti提供可回溯的流量紀錄與查詢
- ✓ 除連線設備納入What's UP軟體管理外，針對連線單位重要設備也納入管理
- ✓ 環境異常通報簡訊化

區網中心服務特色

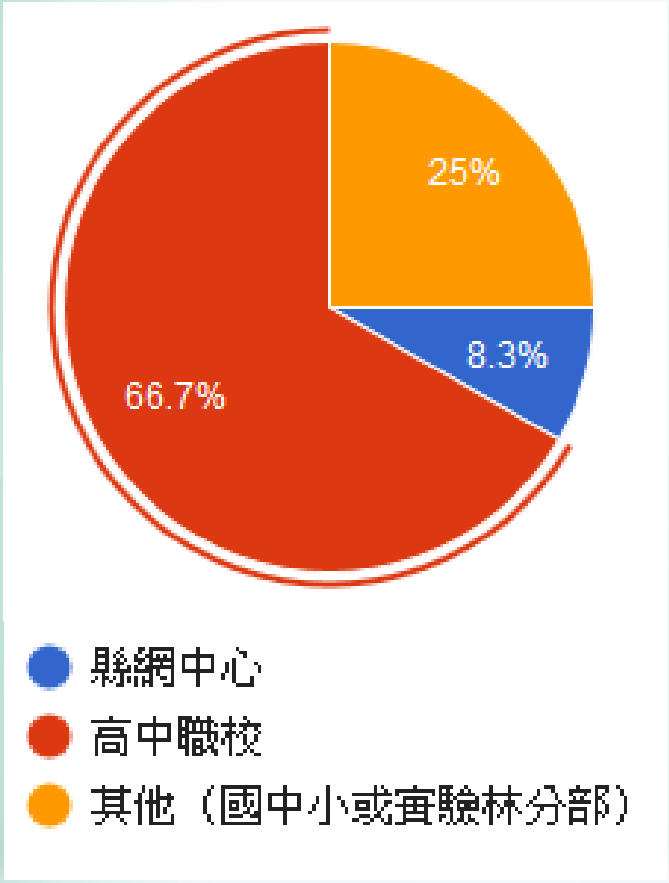
未來服務工作目標

✓ 規劃中的綠能機房碳平衡計畫

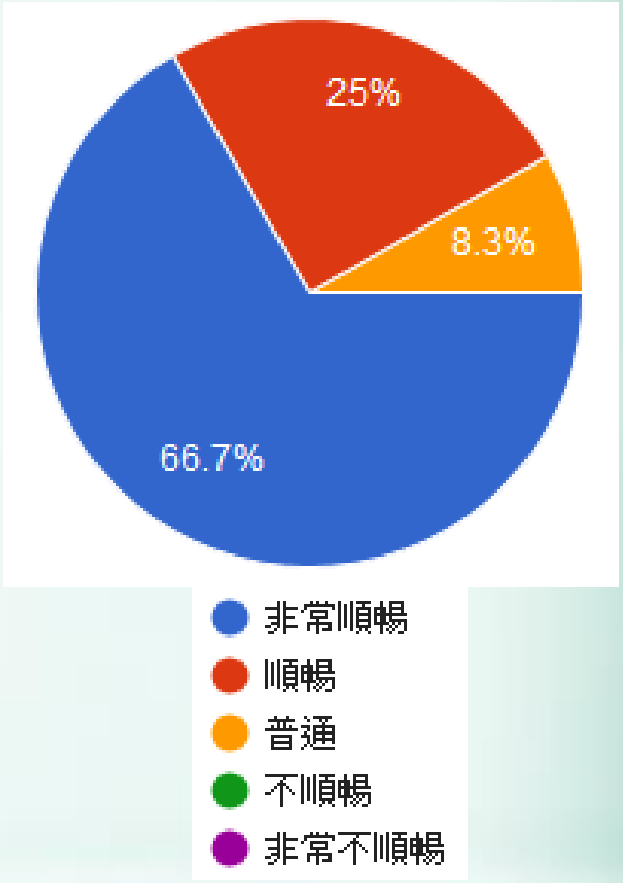
目前區網網路機房每小使用約30kw/h，預計規劃建置200kw的太陽能發電系統，每日發電量800kw做為機房碳平衡計畫。

滿意度調查

1.從介接TANet網路服務架構角度，貴校(單位)的機關組織屬性為

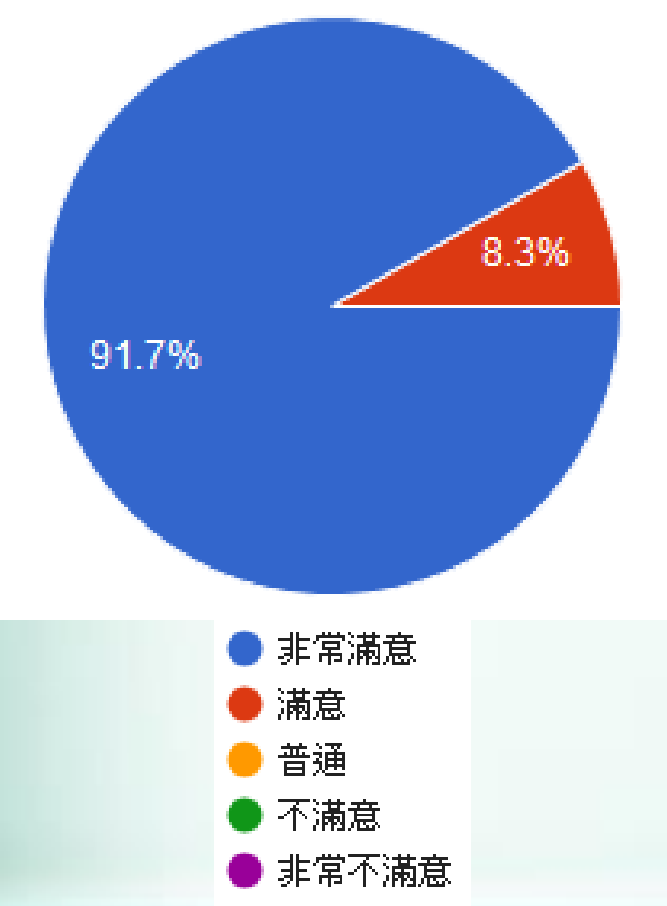


2.本年度區網中心對貴校(單位)之網路連線服務，您認為是否順暢度？

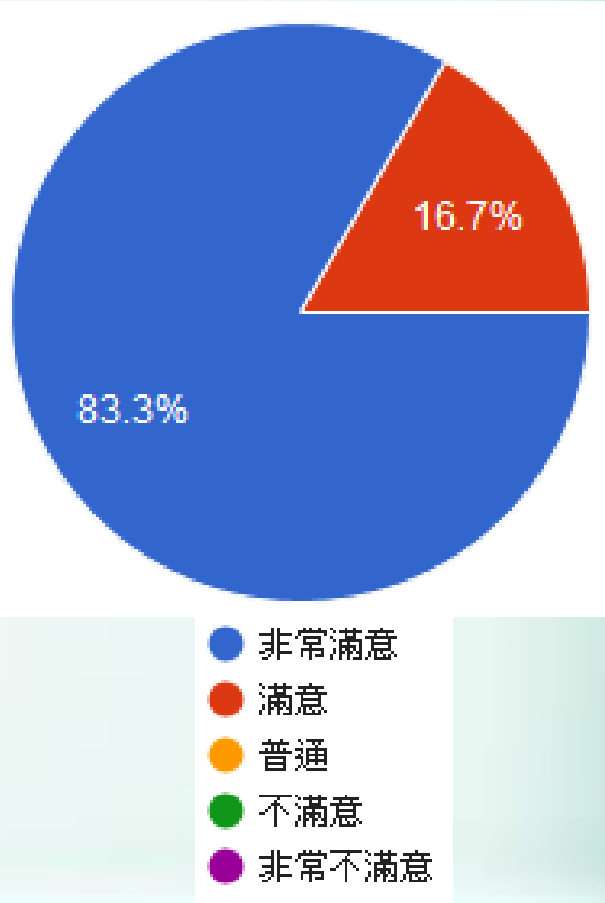


105年度滿意度調查

3.資通安全事件的通報應變協助處理：

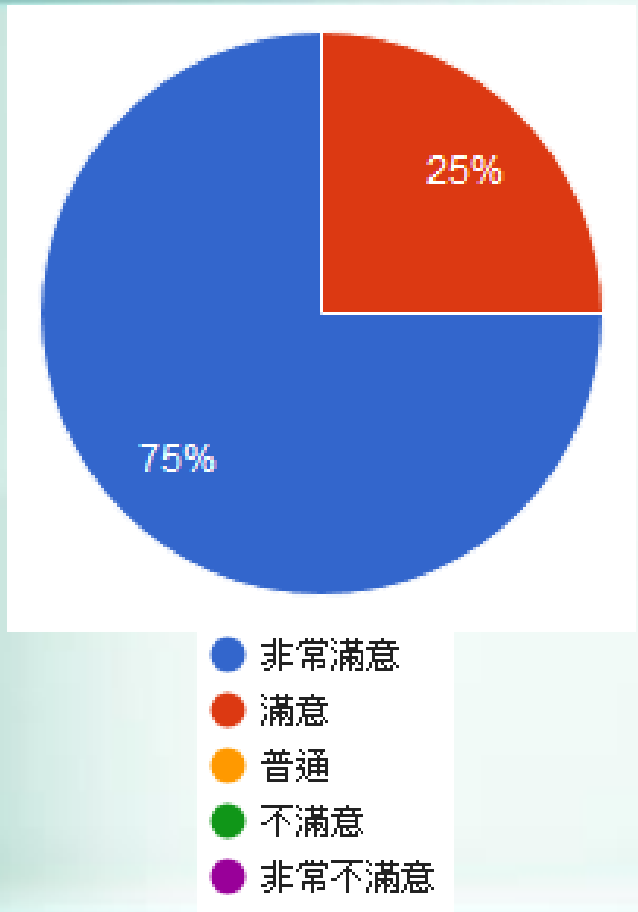


4.網路技術新知的提升上

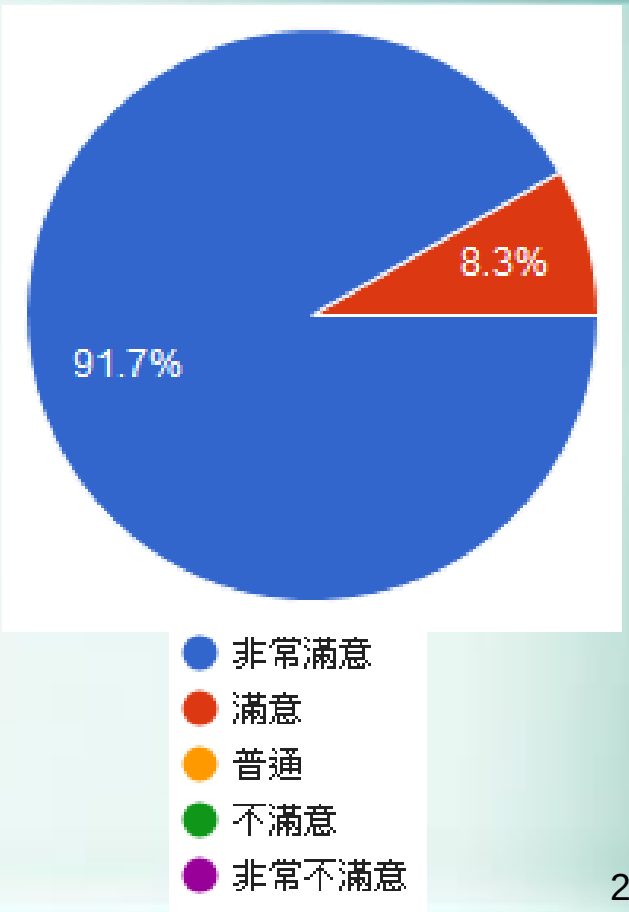


105年度滿意度調查

5.對區網所舉辦之教育訓練或研討(習)課程是否能符合 貴校(單位)實務運作上的需求?

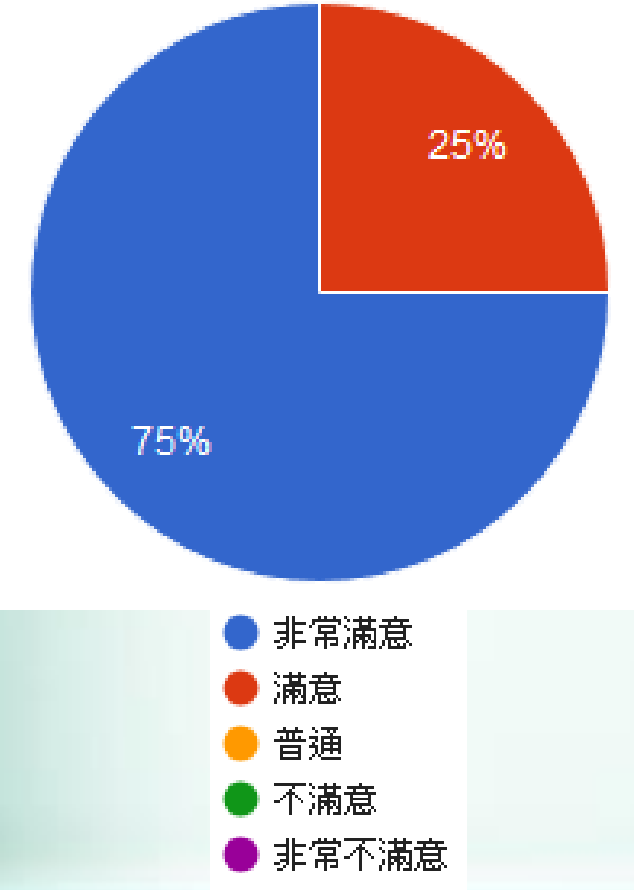


6.貴校(單位)對於區網中心服務人員之熱忱及親和力的滿意度

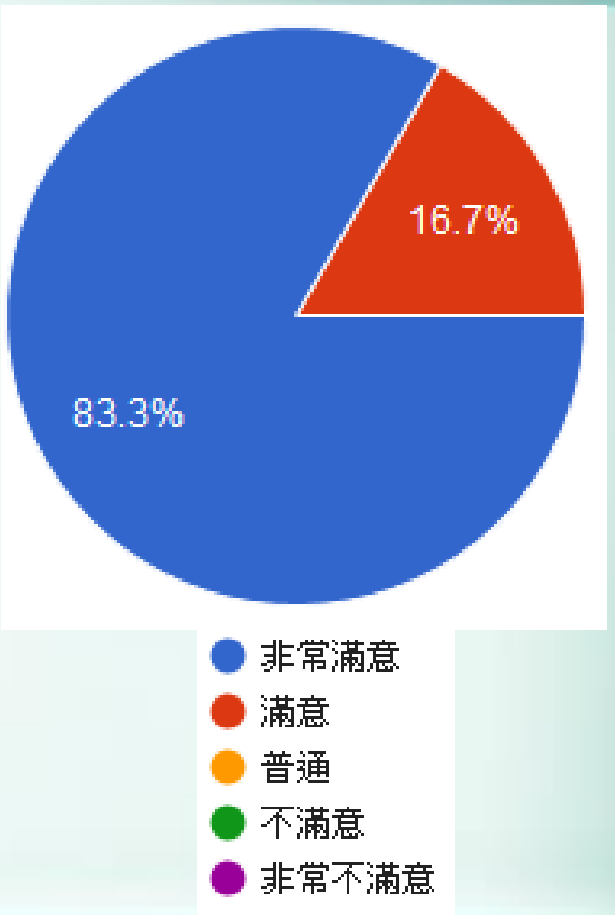


105年度滿意度調查

7.對於區網中心所提供網路維運相關網站的公開資訊， 貴校(單位)是否同意已具備正確性及完整性?



8.貴校(單位)對於區網中心綜合整體服務的表現



簡報結束
謝謝