南投區域網路中心
期末審查

計算機與網路中心 黃育銘主任

報告人：網路組組長 劉震昌

大綱

一、基礎維運資料

（一）經費及人力

（二）基礎資料-網管及資安

1. 區網中心連線資訊彙整表
2. 區網中心資訊安全環境整備表

（三）網管及資安人力服務績效

二、網管策略及具體辦理事項

三、資安服務及政策具體辦理事項

四、特色服務及未來營運

五、前年度改進意見及精進情形

基礎維運

（一）經費及人力-經費使用

1.核定計畫金額：1,390,000

2.教育部補助金額：1,390,000

3.自籌金額：533,000

4.實際累計執行數（至11月）：97%

自籌金額說明:

SMR電力第二迴路接線 23,000

ATS更換 310,000

機房自然進氣系統 200,000

基礎維運

（一）經費及人力-中心人力數

專任：21人　　兼任：2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：6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、網路架設乙級技術士技、CHFI 資安鑑識調查專家認證）

基礎維運(改)

二、網管及資安-連線資訊彙整表

	項目		縣(市)教育網中心	大專院校	高中職校	其他學校	其他單位	總計
(1) 連線數(以單位(校)數統計)	單位(校)數		1	2	9	1	9	22
	連線比例		1/22	2/22	9/22	1/22	9/22	註：單位(校)數 / 總計
(2) 連線頻寬(以電路數統計)	專線							
	光纖	10M(不含)以下		1				1
		10M(含)以上100M(不含)以下					1	1
		100M(含)以上1G(不含)以下			11	1	8	20
		1G(含)以上10G(不含)以下	4	3				7
		10G(含)以上						
	其他(如ADSL等)							
	連線電路小計		4	4	11	1	9	29

台大對高岳營林區

基礎維運(改)

二、網管及資安-連線資訊彙整表

(3)連線縣(市)教育網路中心	縣(市)教育網路中心		連線頻寬(1)	連線頻寬(2)	備註
	1.	南投縣教育處	中華電信1G×2	亞太電信1G×2	
(4)連線其他單位(非ISP)	其他單位名稱		連線頻寬(1)	連線頻寬(2)	備註
	1.	無			
(5)連線TANet及其他ISP線路		臺灣學術網路(TANet)		連線台中主節點頻寬100Gbps	連線台南主節點頻寬100Gbps
(6)補充說明：		無			
(7)連線資訊	請依附表「學校/單位連線資訊詳細表」格式填附				

基礎維運(改)

二、網管及資安-區網中心資訊安全環境整備表

(1)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。(由教育部資科司提供數據)

✓ 1、2級資安事件處理：

(1) 通報平均時數： 0.72小時。

(2) 應變處理平均時數： 0.02 小時。

(3) 事件處理平均時數：0.74 小時。

(4) 通報完成率：100%。

(5) 事件完成率：100%。

(6) 資安事件通報審核平均時數： 0.17小時。

✓ 3、4級資安事件通報：本年度無3、4級資安通報事件

基礎維運

二、網管及資安-區網中心資訊安全環境整備表

（2）網路中心配合本部資安政策。

1. 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：100 %。

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

本中心具備防毒、防火牆、郵件過濾系統、IDS/IPS、Web 應用程式防火牆等設備。

(2)是否符合稽核要求? ■是 □否

本年度6月25、26日通過教版新版 ISMS 稽核

基礎維運

二、網管及資安-區網中心資訊安全環境整備表

(2) 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:

(3)符合資安專業證照人數：8員

本中心陳順德組長、黃景煌資料管理師、藍啟峰技士、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

(4)維護之主要網站進行安全弱點檢測比率：100%。

每年針對連線單位進行兩次校首頁弱點掃描，並將掃描報告分析後，提供給有漏洞的連線單位。

基礎維運

三、網管及資安人力服務績效

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. 舉辦連線單位管理委員會
4. 骨幹網路監測及故障排除
5. 機房環境監測及電力設備維護
6. 提供連線單位技術協助及各事項反應及聯絡窗口
7. 計畫經費控管及承接計畫相關行政流程
8. 配合教育部進行資安通報演練、社交工程演練、業務持續作業演練計畫
9. 阻擋 DDoS 攻擊，降低 DDoS 對網路服務的影響
10. 其他教育部臨時交辦事項

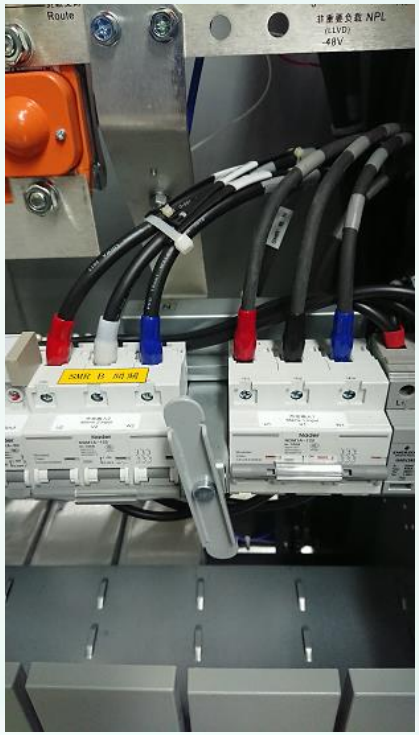
基礎維運

三、網管及資安人力服務績效

11. SMR電力第二迴路接線與ATS更換

SMR A和B 回路開關箱

SMR內部配線，手動切換



基礎維運

三、網管及資安人力服務績效

11. SMR電力第二迴路接線與 ATS 更換

新款控制器，可直接於面板關看目前狀況，也可直接設定參數

基礎維運

三、網管及資安人力服務績效

12.機房自然進氣系統

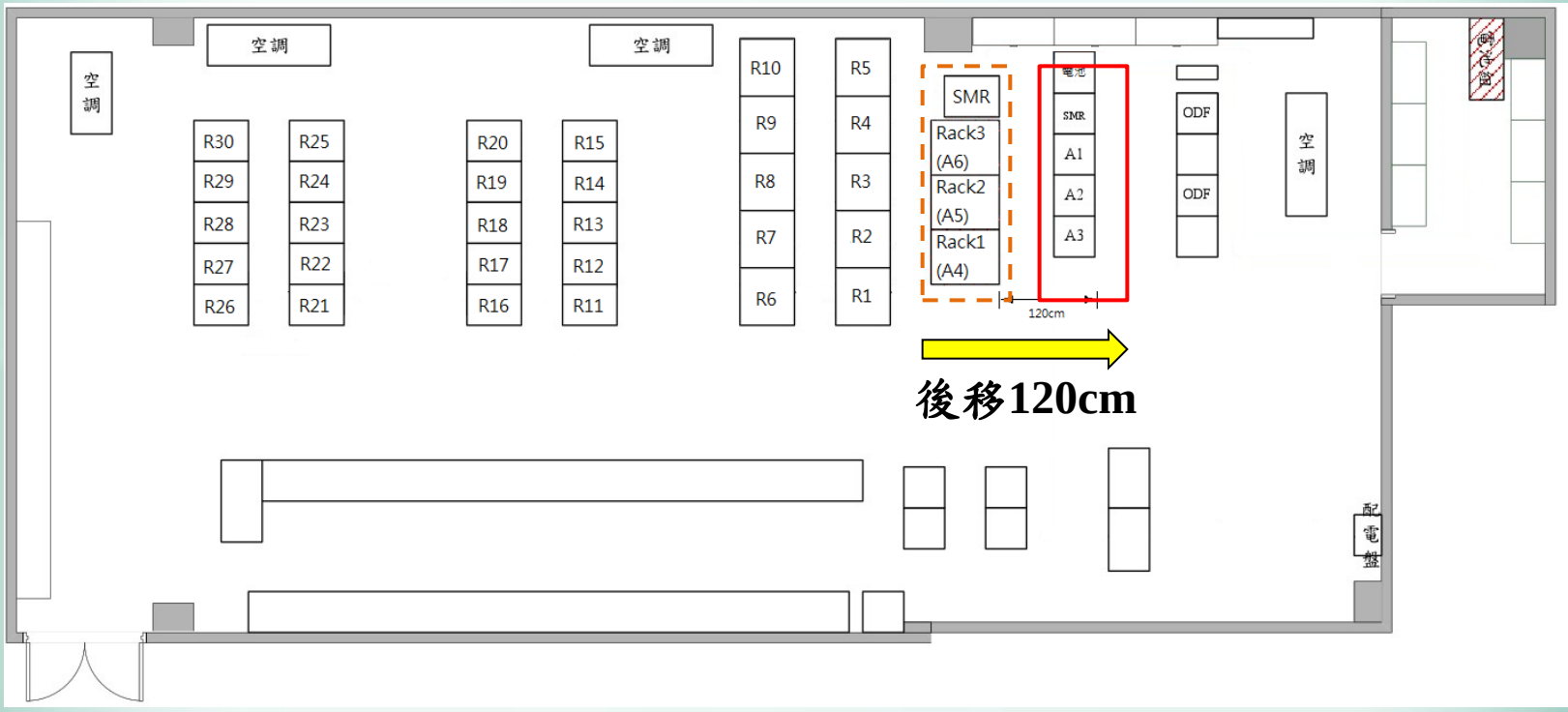
使用更大的風管直接送外氣須要冷卻的區域

5 HP大馬力鼓風機

基礎維運

三、網管及資安人力服務績效

13. 進行骨幹機櫃復位工程



基礎維運

三、網管及資安人力服務績效

13. 進行骨幹機櫃復位工程

- 舊設備移除
- 統計線組是否夠長
- 機櫃固定
- SMR 固定與第二迴路接線

基礎維運

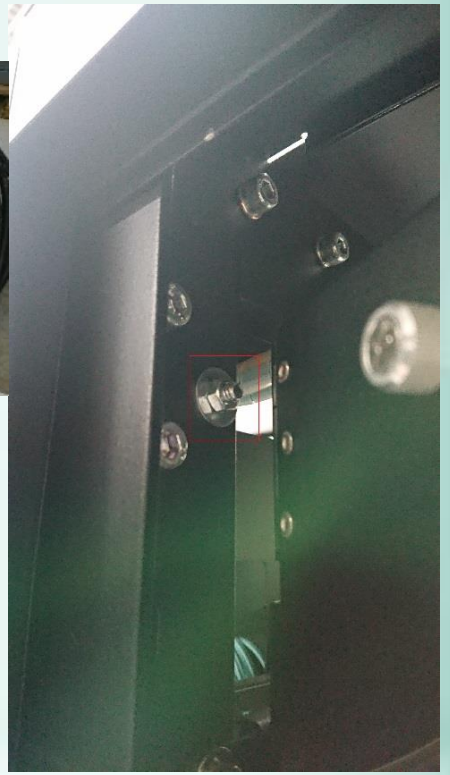
三、網管及資安人力服務績效

13. 進行骨幹機櫃復位工程

拆除原有鋼製底座

補齊高架地板

三個機櫃一同固定



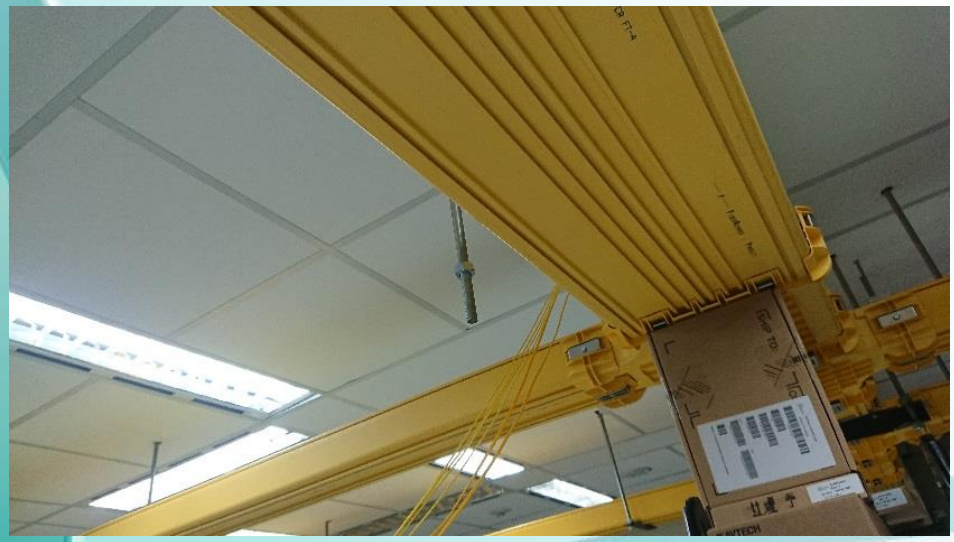
配線盤由R4移到R1

基礎維運

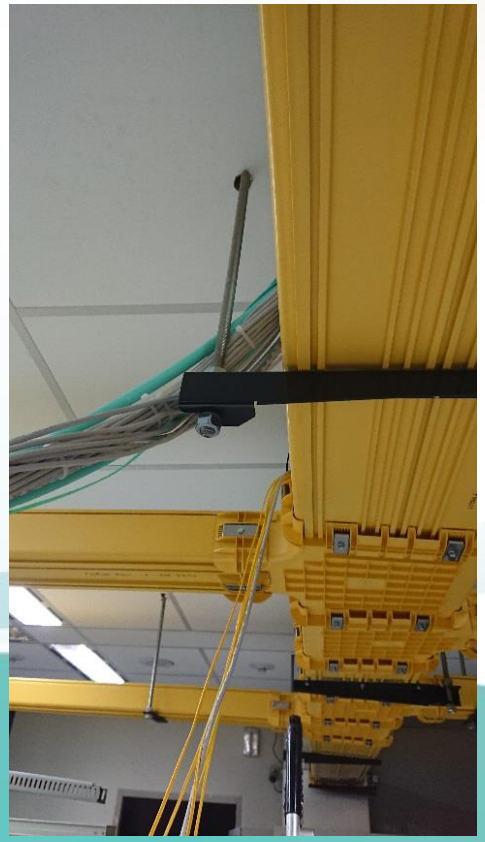
三、網管及資安人力服務績效

13. 進行骨幹機櫃復位工程

拆除固定架，並與以額外支稱以免線槽掉落



線組後移後將固定架鎖回



基礎維運

三、網管及資安人力服務績效

13. 進行骨幹機櫃復位工程

SMR固定於鋼製底座

基礎維運

三、網管及資安人力服務績效

14.舉辦資安教育訓練

本次課程主要為實務操作為主

主題一是弱點掃描平台介紹及實際操作

主題二為 Cacti 軟體建置

貳、網管策略及具體辦理事項

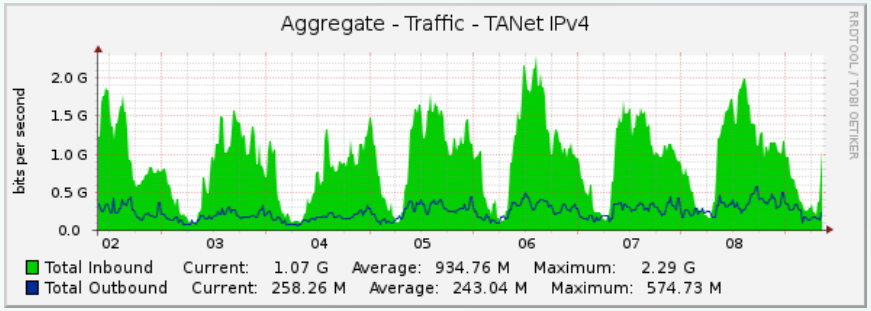
1. VoIP over IPv6 推動：全校已全面改用網路電話系統，已建置 1500 門，皆使用雙協定(IPv4/ IPv6)並將實體 SIP Server 虛擬化。
2. 持續提供 NetFlow 查詢系統並開放給連縣單位使用
3. 持續提供 Cacti 可回溯的流量紀錄與查詢
4. 資安事件：協助查修事件類型及分析，讓連線單位資訊教師能迅速排除問題
5. 實體環境：安裝整合式環境監測系統、並與成功大學異地備份/備援(至 TANet 2018 發表論文-使用 TWAREN VPLS QinQ 實作多重服務異地備份以暨南大學為例)
6. 協助教育部相關計畫：協助遠距課輔硬體及網路維護，及維持課輔品質

貳、網管策略及具體辦理事項

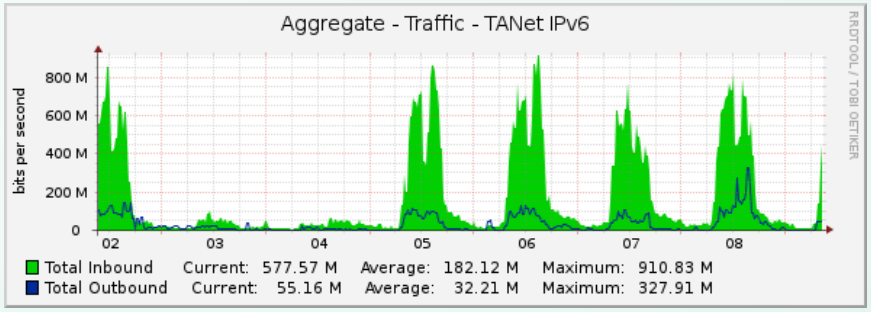
7.下游單位 IPv6 使用狀況分析

IPv4與IPv6比約為2:1

IPv4



IPv6



貳、網管策略及具體辦理事項

8.協助台大實驗林 IP 位置調整與重新分配

新單位的加入但原本配發的 IP無法再切割，與網管負責人討論後把沒用到的網段回收後配給新的單位使用

單位	網段	起始	結束	host數量
	163.22.186.0/24	163.22.186.0	63.22.186.255	256
台大竹山	163.22.186.0/26	163.22.186.0	163.22.186.63	64
台大溪頭	163.22.186.64/27	163.22.186.64	163.22.186.95	32
台大清水溝	163.22.186.96/27	163.22.186.96	163.22.186.127	32
台大木材利用實習工廠	163.22.186.128/27	163.22.186.128	163.22.186.159	32
台大內茅埔	163.22.186.160/27	163.22.186.160	163.22.186.191	32
台大和社	163.22.186.192/27	163.22.186.192	163.22.186.223	32
台大水里營林區	163.22.186.224/27	163.22.186.224	63.22.186.255	32

單位	網段	起始	結束	host數量
	163.22.181.0/26	163.22.181.0	163.22.181.63	64
台大對高岳營林區	163.22.181.0/27	163.22.181.0	163.22.181.31	32
剩餘	163.22.181.32/29	163.22.181.32	163.22.181.39	8
台大下坪植物園	163.22.181.40/29	163.22.181.40	163.22.181.47	8
剩餘	163.22.181.48/28	163.22.181.48	163.22.181.63	16

參、資安服務及政策具體辦理事項

1. 使用A-SOC Sourcefire 3D8120 防火牆及 Paloalto 5060 頻寬管理
2. 協助連線單位資安通報查修，有效降低資安通報量
3. 連線單位網頁弱點掃瞄服務，每年兩次

參、資安服務及政策具體辦理事項

4. 協助縣網進行可疑Domain封鎖

From Port	To Port	IP Protocol	Application	Action	Rule
53601	53	udp	Win.Trojan.Jadtre	deny	Cert_blacklist_App
55798	53	udp	Win.Trojan.Jadtre	deny	Cert_blacklist_App
59737	53	udp	Win.Trojan.Jadtre	deny	Cert_blacklist_App
62148	53	udp	Win.Trojan.Jadtre	deny	Cert_blacklist_App
11224	53	udp	deepsecu.com	deny	Cert_blacklist_App
13864	53	udp	deepsecu.com	deny	Cert_blacklist_App
58965	53	udp	Win.Trojan.Jadtre	deny	Cert_blacklist_App
21597	53	udp	Win.Trojan.Jadtre	deny	Cert_blacklist_App
57383	53	udp	Win.Trojan.Jadtre	deny	Cert_blacklist_App
63415	53	udp	deepsecu.com	deny	Cert_blacklist_App
64331	53	udp	deepsecu.com	deny	Cert_blacklist_App
54313	53	udp	deepsecu.com	deny	Cert_blacklist_App
33531	53	udp	deepsecu.com	deny	Cert_blacklist_App
10944	53	udp	Win.Trojan.Jadtre	deny	Cert_blacklist_App
63736	53	udp	Win.Trojan.Jadtre	deny	Cert_blacklist_App
34438	53	udp	deepsecu.com	deny	Cert_blacklist_App
26568	53	udp	deepsecu.com	deny	Cert_blacklist_App
56405	53	udp	Win.Trojan.Jadtre	deny	Cert_blacklist_App
57740	53	udp	Win.Trojan.Jadtre	deny	Cert_blacklist_App
13875	53	udp	deepsecu.com	deny	Cert_blacklist_App

針對有問題的 Domain Name查詢
直接封鎖，不管 Client 端設定為內部 DNS 或外部 DNS皆可封鎖

```
伺服器:  academic.ncnu.edu.tw
Address:  163.22.2.1

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** 對 academic.ncnu.edu.tw 的要求逾時
>
```

```
> deepsecu.com
伺服器:  one.one.one.one
Address:  1.1.1.1

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** 對 one.one.one.one 的要求逾時
```

參、資安服務及政策具體辦理事項

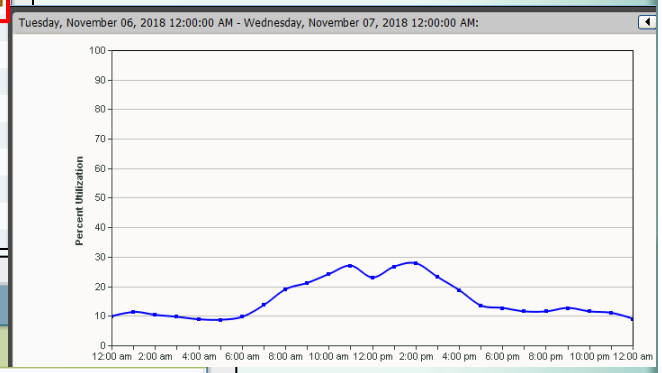
5. 針對 DDoS 攻擊持續調整規則並阻擋攻擊

11/6 9:55～10:55 DoS 攻擊 一小時內被攔截 6.2M 次

Session Limit 於平時上班時間約為 800k 上下

攻擊期間防火牆 CPU 使用率正常連外網也不受影響

	Severity	Threat/Content Name	ID	Threat/Content Type	Count
1	INFORMATIONAL	Session Limit Event	8801	flood	6.2 M
2	CRITICAL	UDP Flood	8502	flood	45.7 K
3	MEDIUM	DNS ANY Queries Brute Force DOS Attack	40033	vulnerability	6.1 K
4	MEDIUM	Suspicious DNS Query (None:beacon.tingyun.com)	404...	spyware	1.6 K
5	INFORMATIONAL	HTTP OPTIONS Method	30520	vulnerability	691
6	LOW	Morto RDP Request Traffic	13274	spyware	521
7	INFORMATIONAL	HTTP Non RFC-Compliant Response Found	32880	vulnerability	258
8	INFORMATIONAL	NetBIOS nbtstat query	31707	vulnerability	201
9	MEDIUM	Suspicious DNS Query (None:lumtest.com)	407...	spyware	185
10	CRITICAL	ZeroAccess.Gen Command and Control Traffic	13235	spyware	123



Top Attackers

	Attacker IP	Attacker Hostname	Attacker	
1	205.205.150.28	205.205.150.28		2.0 M
2	14.135.120.28	14.135.120.28		2.0 M
3	51.15.16.127	51-15-16-127.rev.poneytelecom.eu		1.2 M
4	193.106.31.170	193.106.31.170		627.6 K
5	77.72.82.39	77.72.82.39		129.4 K
6	122.228.19.79	122.228.19.79		44.1 K
7	222.186.31.29	222.186.31.29		41.0 K
8	222.186.172.42	222.186.172.42		36.2 K
9	218.26.94.150	150.94.26.218.internet.sx.cn		27.7 K
10	205.185.122.104	,		11.9 K

參、資安服務及政策具體辦理事項

6. 五育資安事件處理

9/26 接到縣網反應五育高中正在攻擊縣網 DNS，當下與五育老師連繫，但老師表示剛接任此工作約一個月，對於設備位置與設定並不熟悉，並且沒有維護廠商，故與老師約定 9/28 到場協助處理。

VM主機				
HP DL380 G6		163.		
	Doc_BK			
	Doc_New	163.	公文主機	
	Library	無盾		
	Win-V30TC8BL765	無盾		
ASUS RS100		163.		
	common	163.	?	
	www	163.	學校網站	
	eip	無盾		
Dell R610		163.		
	1ligtplus(ubuntu 12.04)(12)	163.	?	
	2Unifi Controller	192. 163.	無線控制器	1.192 重復 2.Radius 有被標記Power Off 3.在不同張資料內有不同IP
	RadiusServer(14)-130514	192. 163.	帳號認證 Power off	
	school(2008 r2)(3)	163.	校務行政	
	windwos 2008 R2 sp1(10)	163. 10.9	備用VM Power off	
	5wuyu-DNS(2003)(1)	163.	DNS Server	
	CentOS6.4(備用)(15)	無盾		

- DNS 設定調整
- 設備位置清查
- VM Server 內 Guest OS 清查

肆、特色服務及未來營運

1. 協助連線單位資安通報查修
2. 協助遠距課輔硬體維護，及維持網路品質
3. 汰換但狀態良好之設備贈與連線單位或其境內國中小(五育、台大實驗林)
4. 自然進氣系統納入環境監測系統統一管理
5. 提供連線單位健檢服務(五育、崇德、力行國小)
6. 預計採購防火牆

伍、前年度改進意見及精進情形

Q1：由區網網站之資料，去年及今年之管理委員會皆只召開一次會議，建議爾後每半年召開一次，並設定好的議題已讓連線單位有意願參與，共同建置優質網路環境。

A1：今年管委會於2月7日舉辦一次，並預計於年終審查後再召開一次。

Q2：建議將區網中心人力資訊呈現於區網中心網頁，以利聯繫和溝通。

A2：感謝委員指正，已更新於區網網頁-業務執掌項下。

伍、前年度改進意見及精進情形

Q3：建議區網中心公告可提供更即時之資訊，並將過期之資訊移置歷史區。斷線公告如果係過期之資料，亦建議移置歷史區域。

A3：網頁已有不定時更新資安相關訊息及漏洞更新訊息。

Q4：建議開放所建置之Cacti系統提供歷史流量查詢功能。

A4：已開放-於區網網頁-網管資訊-

骨幹流量、縣教育網路及大專院校即時流量、高中職校即時流量、國中小及實驗單位即時流量連結內呈現。

伍、前年度改進意見及精進情形

Q5：建議區網中心持續推動IPv6連線支援能力，並將IPv6連線概況呈現於區網中心網頁。

A5：於區網網頁-服務量化指標呈現

Q6：建議將區網中心所提供各項服務之成效(量化數據)呈現於區網中心網頁。

A5：於區網網頁-服務量化指標呈現

伍、前年度改進意見及精進情形

Q7：建議強化辦理教育訓練課程，並將課程以數位影音方式加以留存，以利資訊分享。

A7：舉辦兩場次實作教育訓練課程，課程簡報已放置區網網頁-研討會資訊項下，另如徵得講者同意將會將影音放置網頁分享。

Q8：區網本身之研發能力較不足，建議可參考引進其他區網好的服務或軟體，來供連線單位使用。

Q9：對連線學校的服務可以更精進，服務學校數不多及地域廣大的條件下建議可以和宜蘭大學或東華大學的到府服務交換經驗。

A8、A9：以上建議我們虛心接受，將找機會多與其他區網交流。

簡報結束
謝謝