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）網路中心經費使用

（二）網路中心人力

二 網管及資安

（一）策略及具體完成事項

（二）連線管理策略完成事項

（三）各項基礎資料

三 網管及資安人力運用

四 服務特色

（一）目前服務工作成效

（二）未來目標

區網基礎維運

網路中心經費使用

核定計畫金額：1,471,000

教育部補助金額：1,471,000

實際累計執行數（至11/30）：99.03

自籌金額：1,392,800

- ✓ 核心骨幹路由器與骨幹核心交換器維護費 355,000
- ✓ 虛擬伺服器服務主機 180,800
- ✓ 虛擬化軟體 457,000
- ✓ 虛擬伺服器儲存資料設備 400,000

區網基礎維運

網路中心人力數

專任：19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）

網管及資安

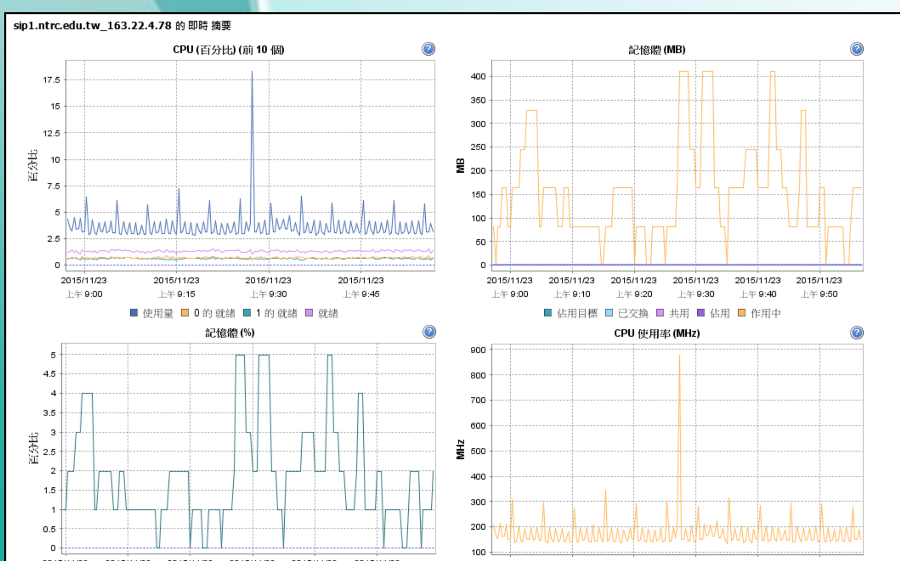
單位策略及具體完成事項-IPv6推動

- ✓ 協助連線單位推動IPv6，區網端IPv6完成率已達100%，隨著連線單位設備的汰舊換新，逐步協助連線單位完成IPv6之設定，今年協助完成的學校有埔里高工、水里商工、暨大附中、仁愛高農、均頭國中等連線單位。

網管及資安

單位策略及具體完成事項- VoIP 推動及成效

- ✓ 推廣VoIP之成效：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)網路。
- ✓ 並將實體SIP Server主機虛擬化
- ✓ 由區網架設SIP主機供連線單位使用
  2015/1~2015/9 通話時間 8094分 通數4762通



SIP Server主機使用量

年	月	累計時間
2015	1	891.5833
2015	2	482.1
2015	3	1086.8
2015	4	884
2015	5	916.1333
2015	6	1057.65
2015	7	931.3333
2015	8	811.55
2015	9	1033.117

通話時間

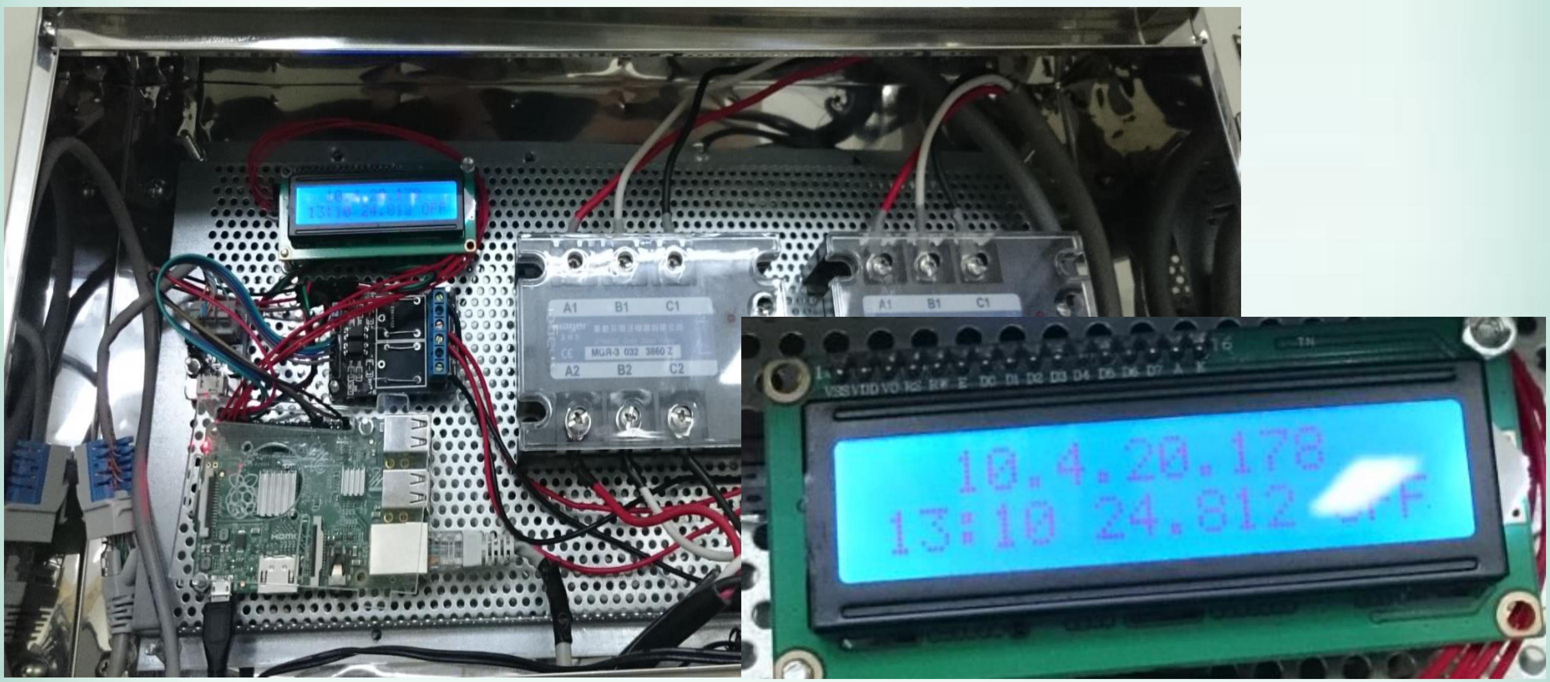
年	月	通數
2015	1	831
2015	2	421
2015	3	649
2015	4	442
2015	5	558
2015	6	571
2015	7	430
2015	8	332
2015	9	528

每月通數

網管及資安

單位策略及具體完成事項-自然進氣系統

- ✓ 系統於戶外氣溫低於21度時開啟自然進氣系統，高於22度自動關閉自然進氣系統



網管及資安

單位策略及具體完成事項-提供VM主機及異地備援

- ✓ 1.提供同德家商VM主機架設圖書查詢系統
- ✓ 2.提供南投縣教育網路異地備源實體空間
- ✓ 3.提供縣網境內國中小網頁空間

Name	State	Host	Provisioned Space	Used Space	Host CPU - MHz	Host Mem - MB	Guest Mem - %
tdvs-104052001 - 163.22.17.148	Powered On	taotie.ncnu.edu.tw	40.00 GB	26.77 GB	2878	4126	14
tdvs-104052003 - 163.22.17.150	Powered On	bixi.ncnu.edu.tw	40.99 GB	10.70 GB	0	1433	0
tdvs-104052002 - 163.22.17.149	Powered On	bixi.ncnu.edu.tw	40.00 GB	17.09 GB	1411	1219	71

Name	State	Host	Provisioned Space	Used Space	Host CPU - MHz	Host Mem - MB	Guest Mem - %
NTNC-1030716 - 163.22.17.104	Powered On	chiwen.ncnu.edu.tw	4.00 TB	6.67 GB	0	767	0

網管及資安

連線管理策略完成事項-網路管理機制

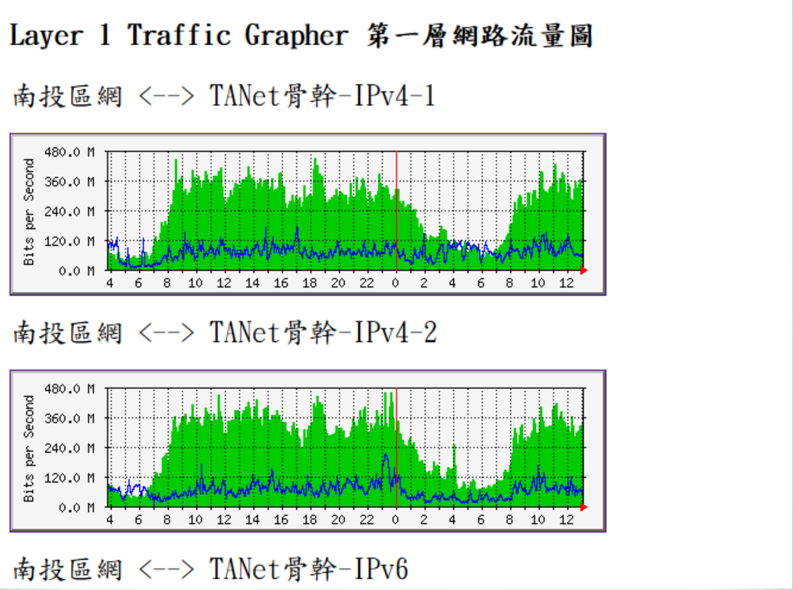
- ✓ 使用MRTG繪製流量圖供下游單位查尋
- ✓ 使用the dude監測軟體確認區網設備使用狀態
- ✓ 使用Mobile One Time Password:一次性密碼
- ✓ 使用A-SOC Sourcefire 3D8120防火牆及Paloalto 5060頻寬管理
- ✓ 加裝Paloalto 5060頻寬管理by pass設備，降低防火牆故障衝擊
- ✓ 協助連線單位資安通報查修，有效降低資安通報量

網管及資安

連線管理策略完成事項-網路管理機制

✓ 使用Mobile One Time Password:一次性密碼

✓ **MRTG繪製流量圖**



✓ **使用the dude監測設備可發出警報**

網管及資安

連線管理策略完成事項-網路管理機制

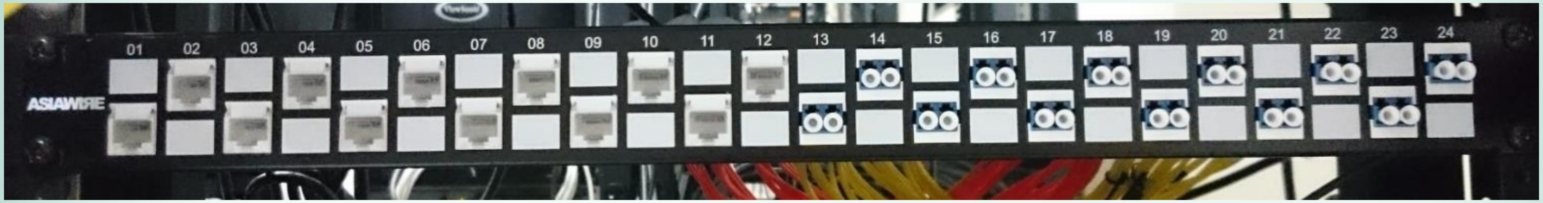
A-SOC Sourcefire 3D8120防火牆

Paloalto 5060頻寬管理

網管及資安

連線管理策略完成事項-網路管理機制

手動by pass面版
自動by pass設備(針對Tanet 2G骨幹)

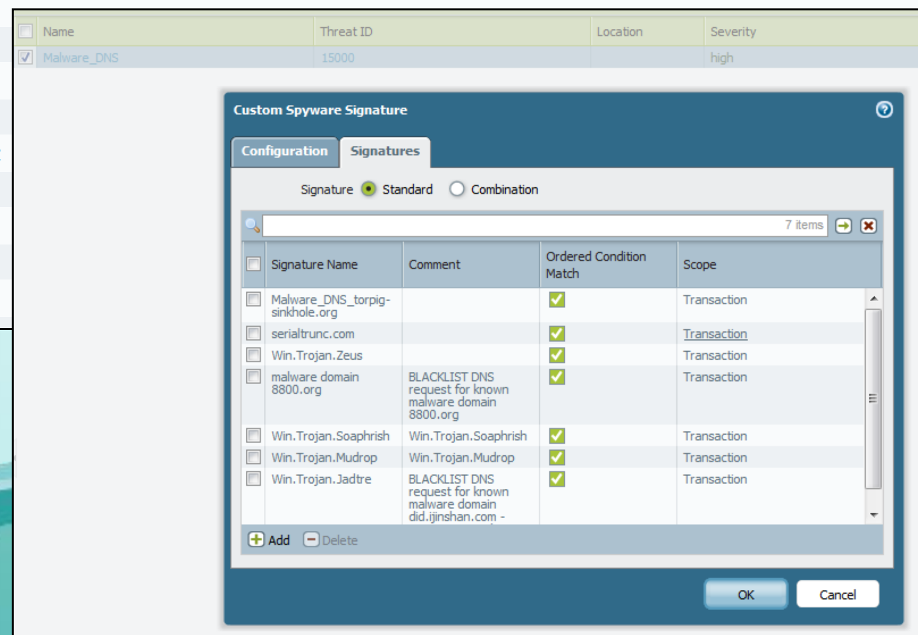


網管及資安

連線管理策略完成事項-網路管理機制

防火牆阻擋攻擊事件

	Threat/Content Name	ID
1	Session Limit Event	8801
2	DNS ANY Queries Brute-force DOS Attack	40033
3	NetBIOS nbtstat query	31707
4	Unknown	15000
5	Sipvicious.Gen User-Agent Traffic	13272
6	DGA NXDOMAIN response Found	40040
7	SCADA Modbus Overlong Request Packet Abnormal	31652
8	SCADA Modbus Invalid Protocol Header	31648
9	HTTP OPTIONS Method	30520
10	UDP Flood	8502
11	UNIX Portmapper Remote Infomation Retrieving Attempt	32796
12	HTTP Non RFC-Compliant Response Found	32880
13	HTTP Directory Traversal Vulnerability	30844
14	Microsoft Windows win.ini access attempt	30851
15	Morto RDP Request Traffic	13274



網管及資安

各項基礎資料-網路中心連線情形

項目(校數)	大專	高中職	其他	總計	
區網中心連線學校數:	1	9	9	19	
連線方式：ADSL（校）					
專線（校）	1			1	暨南大學
光纖10M（校）		2		2	埔里高工、暨大附中
光纖100M（校）		7	8	15	**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 **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				

網管及資安-各項基礎資料

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

	103年度		104年度
1、2級資安事件	(1)自行通報數：21件。 (2)非自行通報數：538件。 (3)平均通報時數：2.09小時。	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)平均通報時數：0.46小時。
3、4級資安事件	(1)自行通報數：0件。 (2)非自行通報數：0件。 (3)平均通報時數：0小時。	3、4級資安事件	(1)自行通報數：0件。 (2)非自行通報數：0件。 (3)平均通報時數：0小時。
平均時數	平均審核時數：0.35小時。 事件平均處理時數：2.09小時	平均時數	平均審核時數：0.26小時。 事件平均處理時數：0.47小時

通報完成率及事件完成率皆為**100%**

網管及資安

各項基礎資料-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 %。(由教育部參照資安通報演練作業現況提供)

本次演練結果：本中心通報及時率、應變時效率、資料正確率皆達滿分，故獲AB級連線單位49個以下組的第二名。

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：4員

(4)維護之主要網站進行安全弱點檢測比率： 100%。

網管及資安人力如何運用

各項基礎資料-網路中心配合本部資安政策

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

6.機房溫濕度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

服務特色

服務成效

- ✓ 提供同德家商VM主機架設圖書查詢系統
- ✓ 提供南投縣教育網路異地備源實體空間
- ✓ 提供縣網境內國中小網頁空間
- ✓ 協助連線單位資安通報查修

Standard shell interperters won't convert the octal to ascii. However, busybox does:

```
$ echo -e '\147\141\171\146\147\164'
\147\141\171\146\147\164
$ busybox echo -e '\147\141\171\146\147\164'
gayfgt
```

The commands supported by the bot are as follows:

```
Frame 1: 103 bytes on wire (824 bits), 103 bytes captured (8
Ethernet II, Src: JuniperN_58:fb:c0 (78:19:f7:58:fb:c0), Dst
Internet Protocol Version 4, Src:
Transmission Control Protocol, Src Port: 49615 (49615), Dst
Telnet
  Data: /bin/busybox;echo -e '\147\141\171\146\147\164'\r\n
```

開始時間	名稱
2015/11/15 01:59:44	MALWARE-CNC Linux.Backdoor.Flooder outbound telnet connection attempt
2015/11/15 01:59:46	MALWARE-CNC Linux.Backdoor.Flooder outbound telnet connection attempt

服務特色

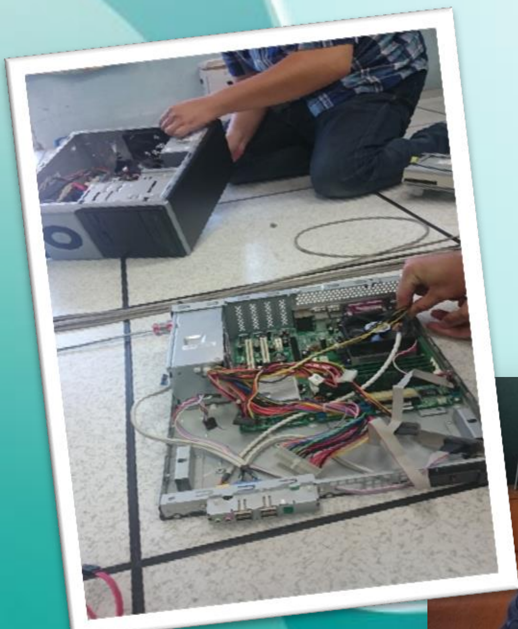
服務成效

- ✓ 預計12/23舉辦開源軟體教育應用研討會
  - 議題一、網路著作權
  - 議題二、從網路開放百寶箱顛覆資訊教育與藝術創作的想像（介紹 OpenClipArt、MuseScore、Blend Swap 等網路百寶箱與自由軟體的應用）
- ✓ 舉辦兩次連線單位管理委員會（2/10、11/13）
- ✓ 今年提供5所高中職網路建檢服務(同德家商、水里商工`台大實驗林水里木材實習場分部、均頭國中、埔里高工）

服務特色

服務成效-協助遠距課輔硬體維護，及維持網路品質

日期	維護小學
104/03/03、104/07/21	東埔國小
104/03/05、104/07/20、104/10/16	力行國小



服務特色

服務成效-協助遠距課輔硬體維護，及維持網路品質

日期	維護小學
104/03/10、104/07/13、104/09/17	北港國小
104/07/16	合作國小、平靜國小




服務特色

服務成效-舉辦2015 TANET 學術研討會

主題演講	主講人
財稅大數據 機會與挑戰	財政部資訊中心 蘇俊榮主任
Cognition-based networks: applying cognitive science to wireless networking	Michele Zorzi （現場備有同步口譯）


服務特色

服務成效-舉辦2015 TANET 學術研討會

與國網中心合作，針對主題演講提供線上直播服務，讓不克前來的人也能不錯過精彩演說

服務特色

服務成效-舉辦2015 TANET 學術研討會

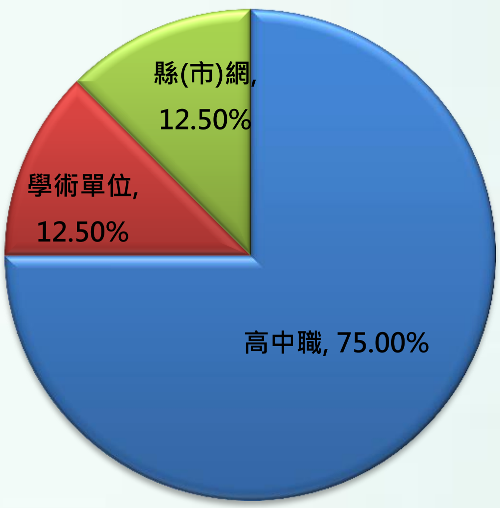
- ✓ 本次投稿共227篇，提供21個最佳論文獎項，每一獎項5000千元，希望鼓勵各位師生及研究人員踴躍投稿
- ✓ 與埔里在地產業及美食小吃提供特色攤位，參加者每人領有50元消費卷，可憑卷至攤位消費

未來目標

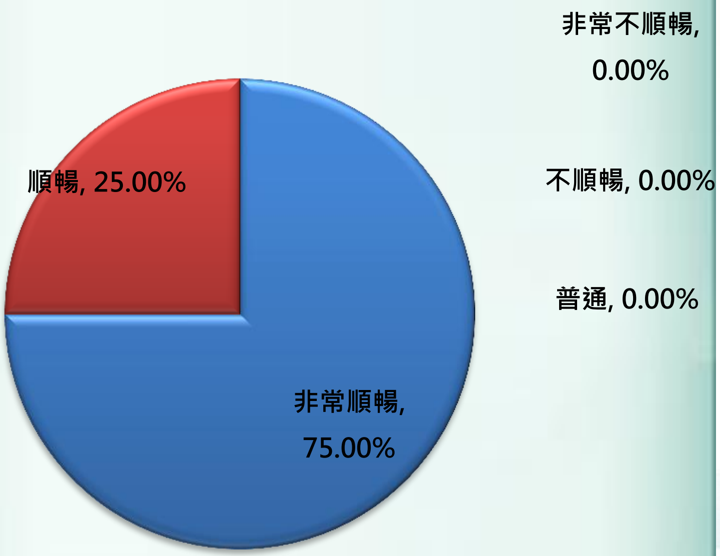
- ✓ 持續推動IPv6，並協助連線單位設定IPv6及測試。
- ✓ 持續維護區網架設之SIP Server，供連線單位使用。
- ✓ 提供VM主機供連線單位申請使用。
- ✓ 舉辦2次連線單位管理委員會。
- ✓ 舉辦一場資安或開源軟體研討會。
- ✓ 持續連線單位資安健檢服務。
- ✓ 協助遠距課輔硬體維護及維持網路品質。
- ✓ 協助連線單位資安通報查修。
- ✓ 針對連線單位建置the dude監測軟體

南投區網連線單位服務滿意度問卷結果

從介接TANet網路服務架構角度，
貴校(單位)的機關組織屬性為：

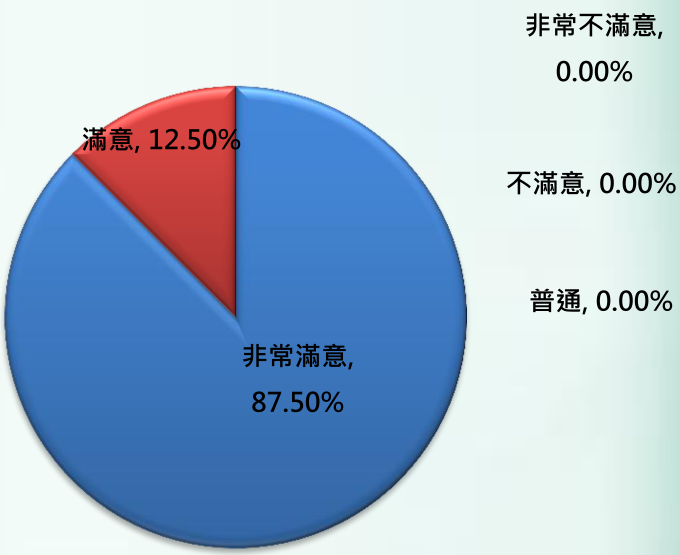


本年度區網中心對　貴校(單位)之網路連線服務，您認為是否順暢度？

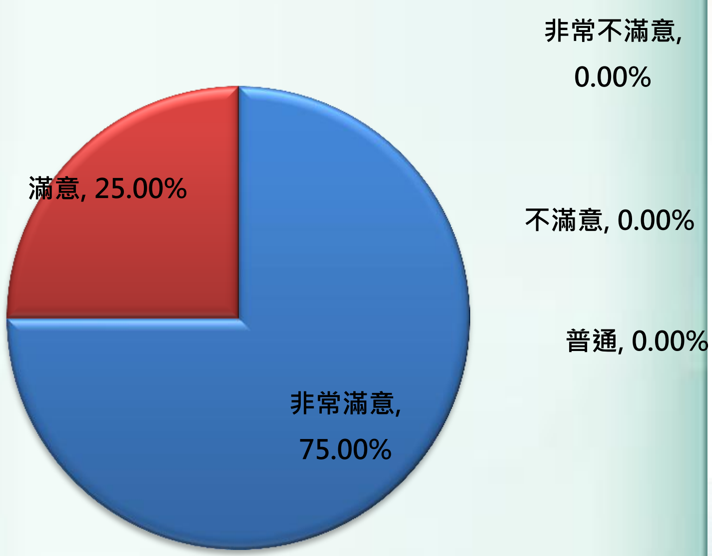


南投區網連線單位服務滿意度問卷結果

資通安全事件的通報應變的協助處理：

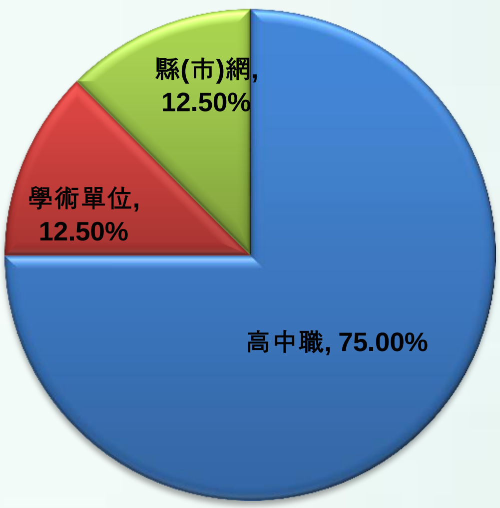


網路技術新知的提升上：

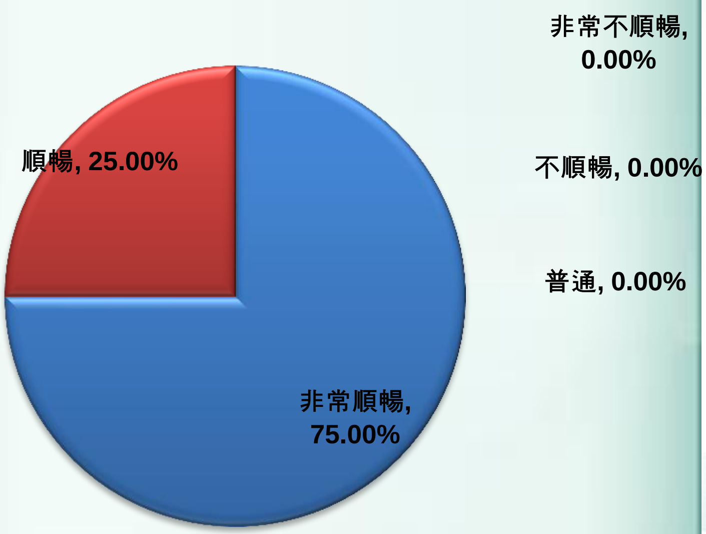


南投區網連線單位服務滿意度問卷結果

從介接TANet網路服務架構角度，貴校(單位)的機關組織屬性為：



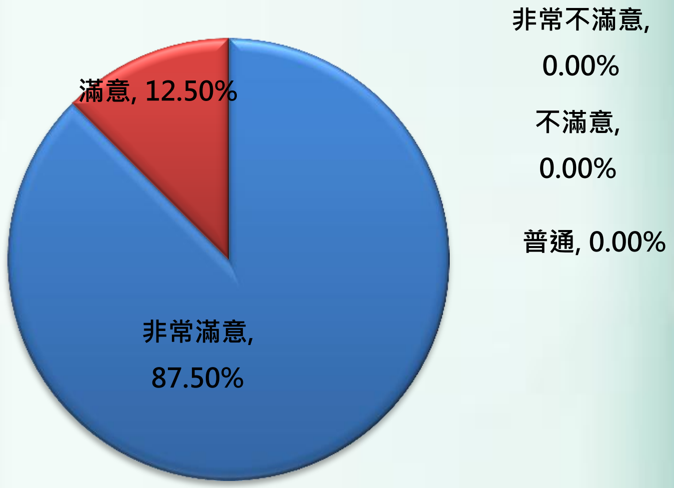
本年度區網中心對　貴校(單位)之網路連線服務，您認為是否順暢度？



南投區網連線單位服務滿意度問卷結果

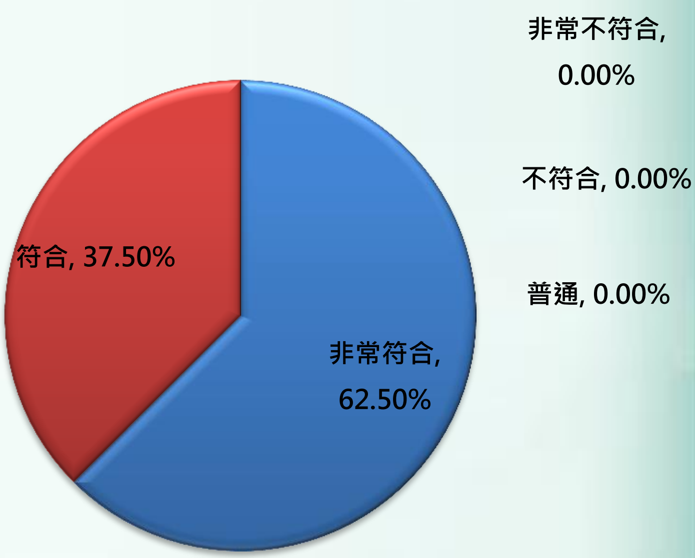
聯繫協調與溝通管道上：

對臺灣學術網路之相關政策(如:資安、網路智財權、網路管理、資訊素養、網路應用服務等)，區網中心是否能充分向　貴校(單位)說明：

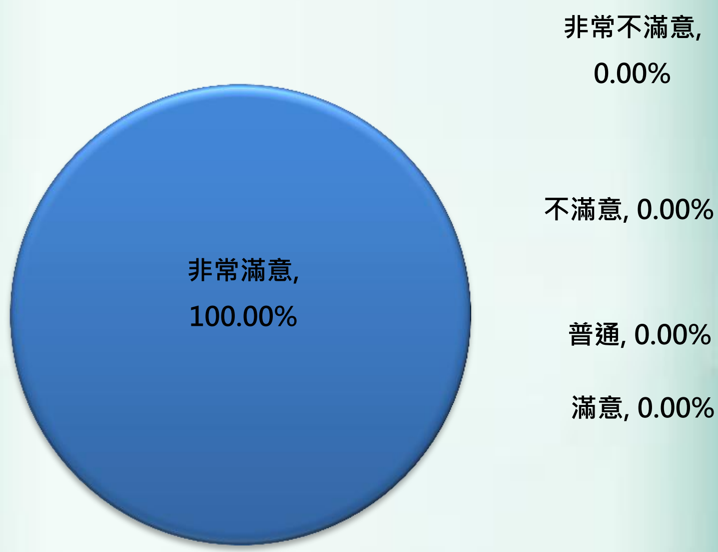


南投區網連線單位服務滿意度問卷結果

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?

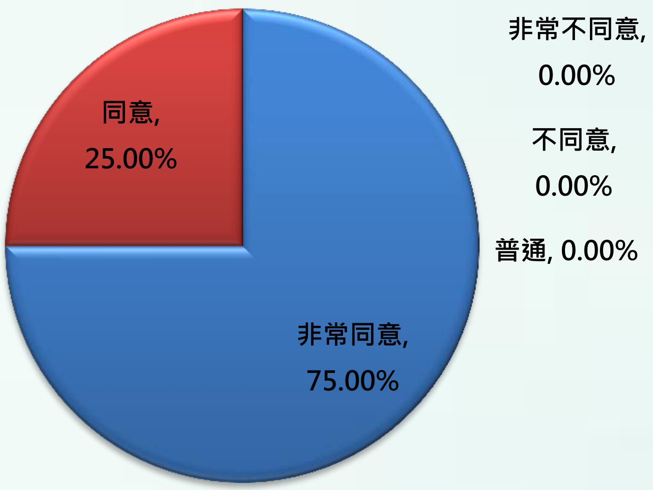


貴校(單位)對於區網中心服務人員之熱忱及親和力的滿意度？



南投區網連線單位服務滿意度問卷結果

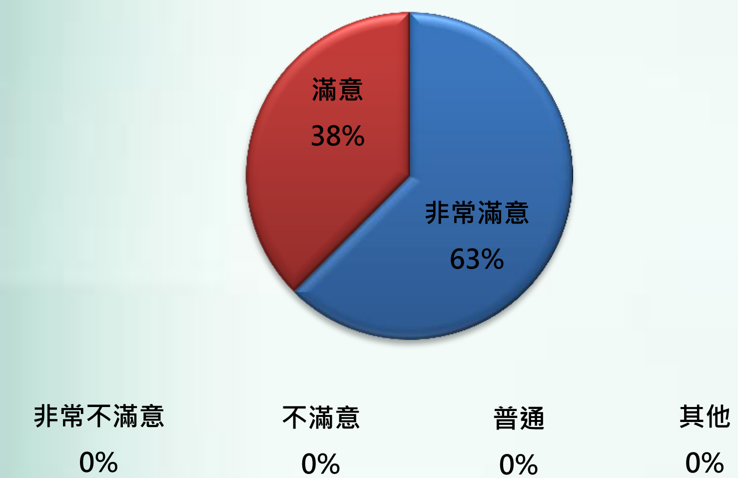
對於區網中心所提供網路維運相關網站的公開資訊， 貴校(單位)是否同意已具備正確性及完整性？



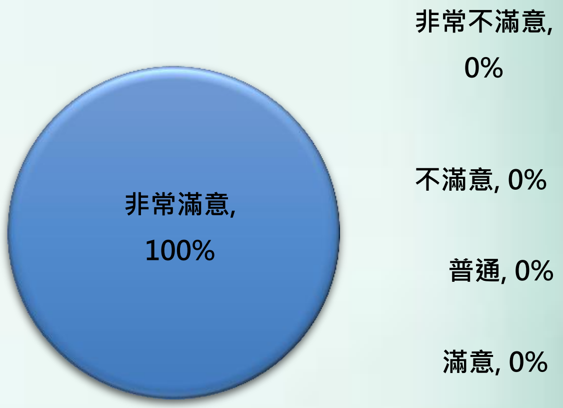
南投區網連線單位服務滿意度問卷結果

貴校(單位)對於區網中心綜合整體服務的表現

103年

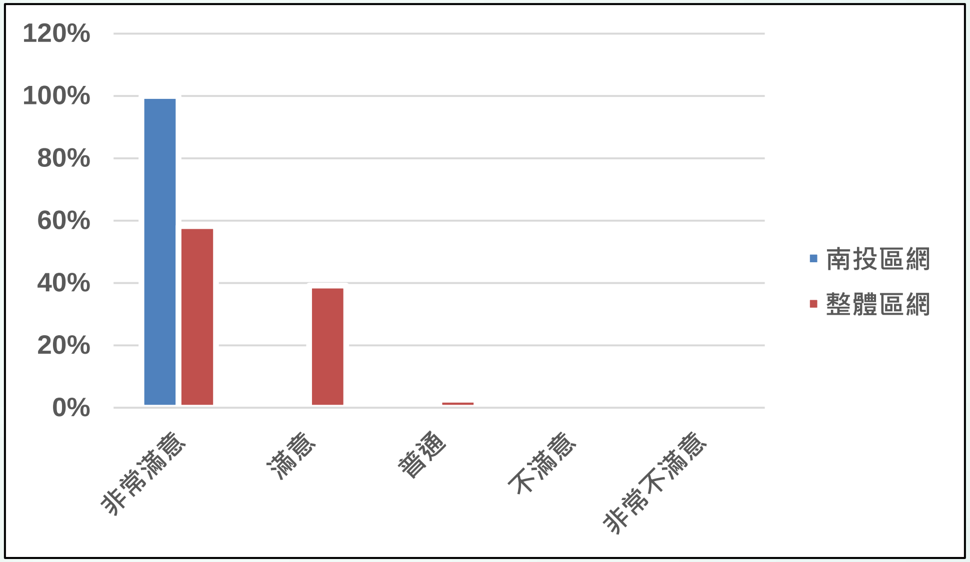


104年



南投區網連線單位服務滿意度問卷結果

貴校(單位)對於區網中心綜合整體服務的表現



南投區網連線單位服務滿意度問卷結果

✓ 在網路管理方面，您目前(或曾經)遭遇最大的困難？

1.人力不足。因僅由學校設備組兼管。

2.區網中心對本單位之網路連線服務順暢，但是它的出口僅國家高速網路中心及教育部（實際上就是只有教育部出口），而塞車最主要也在教育部出口，所以對區網中心順暢，並不代表網路順暢。

3.學校不重視。

✓ 對區域網路中心在網路維運管理的建議

1.如果區網中心能代勞管理IDS，或是主動阻擋一些攻擊事件，可以減輕縣網的工作。

2.很讚。

✓ 對臺灣學術網路運作的整體建議

1.可以再多一點經費給下游學校，增建設備以提供更好的服務給學生！

2.建議教育部或區網中心能多提供下車的ISP線路，減少本縣因位於網路末端，對於上游造成網路中斷或塞車的現象，以免變成一座網路孤島。

3.降低學校連接區網之費用

4.費用太貴。

簡報結束
謝謝