TANET竹苗區域網路中心
105年度成效報告

國立交通大學 資訊技術服務中心

(105.11.24)

綱要

1. 網路中心基本資料及人力運作情形
2. 網路中心運作情形
3. 資訊安全環境整備
4. 推動網路資訊應用環境之導入情形
5. 網路應用創新服務情形
6. 辦理教育訓練及推廣活動情形
7. 年度計畫所提績效指標辦理情形
8. 學校對網路中心維運配合款及經費運用情形
9. 結語與綜合建議
10. 106年度預計推動之重點工作

1. 網路中心基本資料及人力運作情形

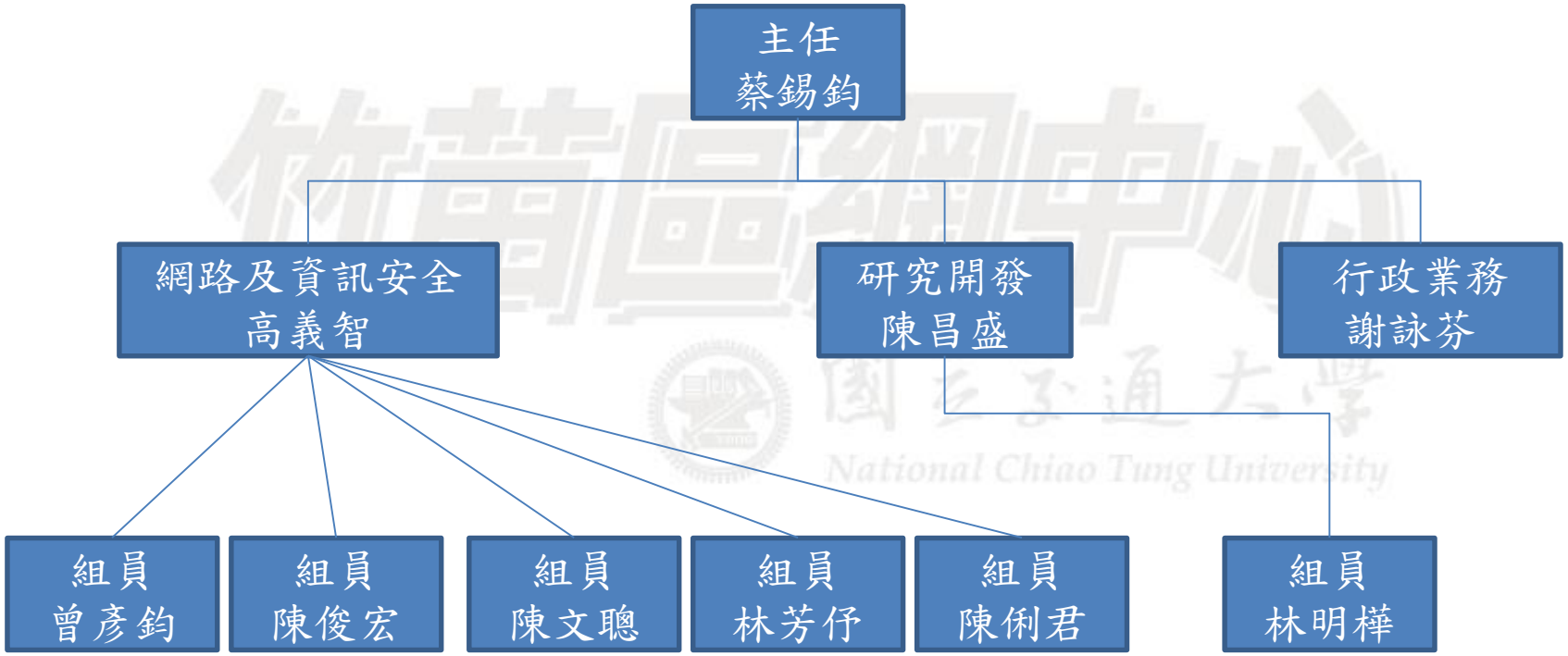
- **單位名稱：竹苗區網中心—國立交通大學**
  - 網址：http://www.hcrc.edu.tw
  - 地址：300新竹市大學路1001號
  - 傳真：03-5714031
- **單位主管：蔡錫鈞 主任**
  - E-mail：sctsai@cs.nctu.edu.tw
  - 電話：03-5731900
- **網路系統組：高義智 組長**
  - E- mail：ykao@mail.nctu.edu.tw
  - 電話：03-5712121#31905
- **網管負責人：曾彥鈞**
  - E- mail：ay529@mail.nctu.edu.tw
  - 電話：03-5712121#52885
  - 手機：0978070580
- **資安負責人：陳俊宏**
  - E- mail：lovetaouc@nctu.edu.tw
  - 電話：03-5712121#31483
  - 手機：0921433247

網路中心基本資料及人力運作情形-cont

- 本區網中心專職與兼任參與維運所投入人力：10人
- 教育部補助款專職人員：2人
- 交通大學資訊技術服務中心：8人

網路中心基本資料及人力運作情形-cont

組織架構圖



網路中心基本資料及人力運作情形-cont

教育部支援網管及資安人力運用

類別	姓名	工作項目
網管人員	曾彥鈞	1.區網網路設備維護設定 2.建立網路監控系統—cacti 2-1 網路頻寬及時流量圖 2-2 各單位頻寬超載或過低警告通知 2-3 每日自動寄出前一日各單位流量趨勢圖至各單位網管 3.協助各單位建立Ipv6網路環境 4.竹苗區網網頁公告平台建置維護 5.舉辦連線單位教育訓練課程 6.協助連線單位設定網路電話 7.協助連線單位建置單位內網管系統 8.網路異常處理 9.輔導所屬連線單位網路維運管理

網路中心基本資料及人力運作情形-cont

類別	姓名	工作項目
資安人員	陳俊宏	1. ISO27001教版(ISMS)稽核 2. 區網資安設備(Paloalto 5060)設定維護 2-1 定期更新並封鎖TACERT提供之威脅名單 2-2 查看大量異常行為IP並通知單位網管人員 2-3 提供各單位其資安通報IP之相關流量記錄檔 2-4 設定調整防火牆規則 2-5 頻寬使用(QOS)設定整 3. 教育機構防洩漏個資掃描平台維護及審查 4. 應用程式弱點掃描監測平台維護及審查 5. 教育部資安通報處理 5-1 竹苗區網中心資安事件處理人員 5-2 協助連線單位處理資安事件及審核 5-3 提醒連線單位處理資安事件 5-4 協助各單位進行教育部資安演練 6. 協助進行營運持續計畫BCP演練

2. 網路中心運作情形

業務負責人	執掌	職務代理人
•高義智 組長 •ykao@mail.nctu.edu.tw •03-5731905	•綜理TANET業務 •區網中心業務推動 •資安事件協調處理	林芳仔
•陳昌盛 組長 •cschen@mail.nctu.edu.tw •03-5731721	•TANET業務顧問	
•曾彥鈞 •ay529@mail.nctu.edu.tw •03-5712121 #52885	1. 協助TANet區網中心輔導所屬連線單位網路維運管理 2. TANET網路骨幹管理 3.TANET路由管理 4. ISP介接連線管理 5.竹苗區網問題諮詢 6. 各級學校與機關連線事宜	林芳仔
•陳俊宏 •lovetaou@nctu.edu.tw •03-5712121 #31483	1. TANET管理委員會 2. TANET教育訓練 3. 通安全宣導服務 4. 區網中心網站維護 5. 竹苗區網問題諮詢 6. TANET IPv6推動 7.竹苗區網網站弱點掃瞄及防洩漏個資業掃描平台業務	陳文聰
•陳俐君 •lichun80@nctu.edu.tw •03-5712121 #31268	1. TANET ISMS業務維運 2.資訊機房維運相關事項	**陳俊宏**
•謝詠芬 •yongfen@mail.nctu.edu.tw •03-5731702	•處理竹苗區網行政業務	
•林明樺 •mhlin@mail.nctu.edu.tw •03-57312121#31726	1. VoIP推動 2. DNS及Mail相關問題諮詢	

網路中心運作情形-cont

- 105年組織運作網址：
- http://www.hcrc.edu.tw/node/46

網路中心運作情形-cont

- 105年竹苗區網管理委員會網址：
- http://www.hcrc.edu.tw/node/28

關於竹苗區網

- 中心簡介
- 基本聯絡資料
- 人力狀況與業務執掌
- 區網連線單位資訊
- 竹苗區網網路架構
- 管理委員會會議紀錄

臺灣學術網路友站連結

- 資訊及科技教育司
- TANET管理委員會會議紀錄
- TWAREN技術小組會議會議記錄
- 臺北區域網路中心-台大
- 臺北區域網路中心-政大
- 桃園區域網路中心
- 竹苗區域網路中心
- 新竹區域網路中心
- 臺中區域網路中心
- 南投區域網路中心

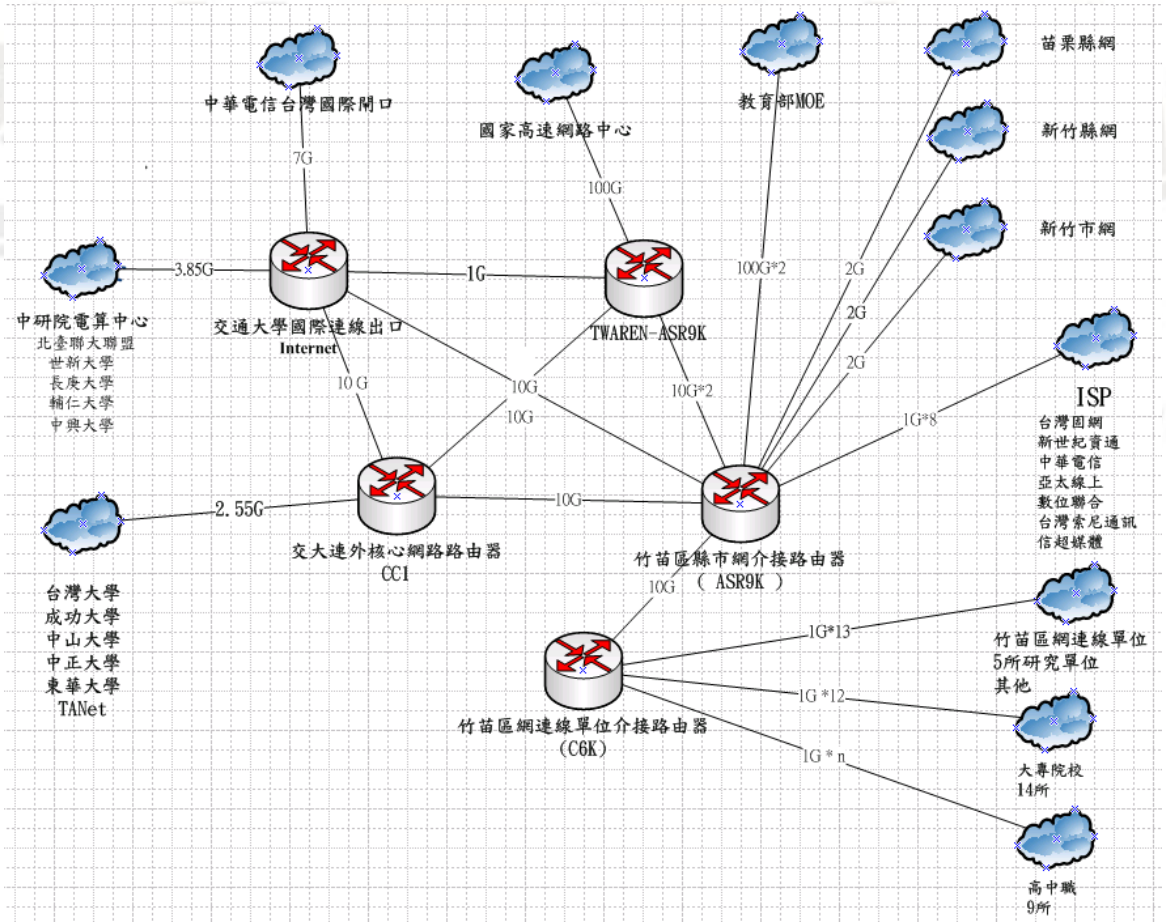
首頁

會議紀錄

民國91年		九十一學年第一次會議
民國92年	九十一學年第二次會議	九十二學年第一次會議
民國93年	九十二學年第二次會議	九十三學年第一次會議
民國94年	九十三學年第二次會議	九十四學年第一次會議
民國95年	九十四學年第二次會議	九十五學年第一次會議
民國96年	九十五學年第二次會議	九十六學年第一次會議
民國97年	九十六學年第二次會議	九十七學年第一次會議
民國98年	九十七學年第三次會議	
民國99年	九十八學年第一次會議	
民國100年	100學年第一次會議	100學年第二次會議
民國101年	101學年第一次會議	
民國102年	102學年第一次會議	102學年第二次會議
民國103年	103學年第一次會議	103學年第二次會議
民國104年	104學年第一次會議	104學年第二次會議
民國105年	105學年第一次會議	105學年第二次會議

網路中心運作情形-cont

- 105年竹苗區網網路拓墣圖網址：
- http://www.hcrc.edu.tw/node/24



3. 資訊安全環境整備-竹苗區網中心通過 ISMS

◆竹苗區網中心 ISMS 導入範圍

1. 機房處理TANet業務活動之運作維護
2. 學籍系統之維護管理

◆已於本年度04月27日完成複評

資訊安全相關服務-竹苗區網中心已達ISO27001國際標準

◆國立交通大學 ISO 27001 導入範圍

1. 機房維運相關人員所提供之資訊機房環境之執行、維護與管理作業流程。

◆已於本年度04月27日完成複評。

3. 資訊安全環境整備-竹苗區網中心通過 ISMS

SGS

Certificate TW12/11622

The management system of

Information Technology Service Center, National Chiao Tung University

1001 University Road, Hsinchu, Taiwan

has been assessed and certified as meeting the requirements of

ISO/IEC 27001:2013

For the following activities

The operation, maintenance and management of the IT server room and Grading System, provided by the Network System Group, related Technology Development Group, and related Academic Information Group. The scope does not include the system development, research and testing on Beta Site, management and service of non-backbone campus network, management of dormitory network, maintenance and management of servers owned by administrative and academic units, and management of PC classrooms. The scope declared above is in accordance with the Statement of Applicability version 2.0.

This certificate is valid from 18 June 2015 until 18 June 2018 and remains valid subject to satisfactory surveillance audits.
Re certification audit due before 14 May 2018
Issue 3. Certified since 18 June 2012

Authorised by

UKAS MANAGEMENT SYSTEMS 0005

SGS United Kingdom Ltd Systems & Services Certification
Rossmore Business Park Ellesmere Port Cheshire CH65 3EN UK
t +44 (0)151 350-6666 f +44 (0)151 350-6600 www.sgs.com
SGS 27001 01 0714
Page 1 of 1

SGS

資訊安全環境整備$_2$-竹苗區網網頁弱點掃描

- **相關網址：http://ewavs.hcrc.edu.tw/（支援IPV6）**
- **已註冊連線人數：50人**
- **已掃瞄成功網站數量：657個網站**
- **已上線掃瞄單位：**

➢ 大專院校: 交通大學、中華大學、聯合大學、陽明大學、亞太創意技術學院、中國科技大學、 玄奘大學、大華技術學院、元培科技大學、新竹教育大學、明新科技大學、育達商業技術學院、中華科技大學、仁德醫護管理專科學校、國立陽明大學附設醫院、。

➢ 研究單位機關 ： 國家系統晶片設計中心，財團法人食品發展研究所、工業技術研究院、國家奈米元件實驗室。

➢ 高中職 ： 曙光高中、新竹高工、苗栗高中、新竹高商、光復高中，新竹高中、世界高中、園區實驗高中、忠信高中、新竹女子高級中學。

資訊安全相關服務3-竹苗區網防洩漏個資掃描平台

- **相關網址：http://epdp.hcrc.edu.tw（支援IPV6）**
- **已註冊連線人數：56個單位**
- **已掃瞄成功網站數量：453個網站**
- **已上線掃瞄單位：**
- 大專院校:玄奘大學、陽明大學、中華大學、元培科技大學、交通大學、新竹教育大學、明新科技大學、育達商業科技大學、聯合大學、亞太創意技術學院、國立陽明大學附設醫院、大華技術學院、中國科技大學、國立聯合大學、中華科技大學新竹分部、仁德醫護管理專科學校等 學校。

➢ 高中職 :新竹高商、新竹市世界高級中學、新竹高工、國立新竹高級中學、國立苗栗高中、曙光女中、私立忠信學校、國立新竹女子高級中學、苗栗高商、光復高級中學、國立科學工業園區實驗高級中學、新竹市建功國小及苗栗照南國小。

➢ 研究單位機關:食品工業發展研究所、國家晶片系統設計中心、國家奈米元件實驗室、工業技術研究院。

資訊安全相關服務4- 智慧財產權保護

校園智慧財產權保護 – 宣導活動

- 推廣資訊安全與網路智財權知識
  - 每學期初針對系所暨行政單位網管人員舉辦「資通安全及連絡人」講習會
- 校園網路智慧財產權法令宣導
  - 建置專屬網頁 ，網址：http://isipr.nctu.edu.tw/，以將此網頁連結放置在竹苗區網網頁中
  - 每學期至少舉辦乙次宣導會，推廣尊重智慧財產權觀念
  - 協同其他單位舉辦相關智財權宣導工作坊與演講
  - 與課務（選課）系統結合，進行智慧財產權宣導
- 舉辦「校園網路智慧財產權有獎徵答活動」
  - 活動目的在透過有獎徵答方式，吸引同學注意並對智財權有更多、更完整之瞭解

4. 推動網路資訊應用環境之導入情形

- Tanet學術網路骨幹100G升級案
- 透過CACTI監控系統監控網路流量
- 協助連線單位導入IPv6
- 網路資訊安全設備

推動網路資訊應用環境之導入情形1

- Tanet學術網路骨幹100G升級案
  - 已建置3個連續櫃D1、D2及D3櫃，分別放置相關設備

櫃位編號	D3	D2	D1
			

推動網路資訊應用環境之導入情形1

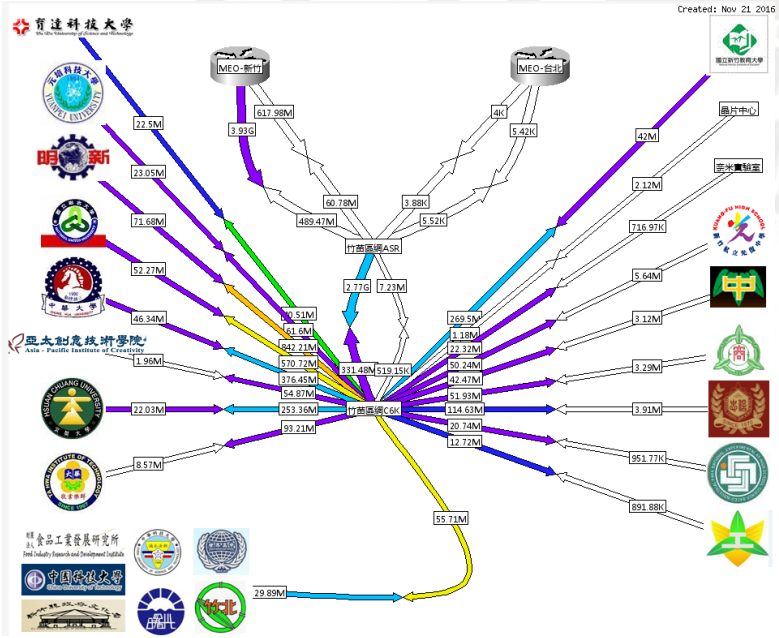
- Tanet學術網路骨幹100G升級案
  - 更新機房空調設備
  - 建置上吹式20頓氣冷型兩座及下吹式20T水冷型主機三座(更新五座冰水主機)
  - 達成互相備援機制

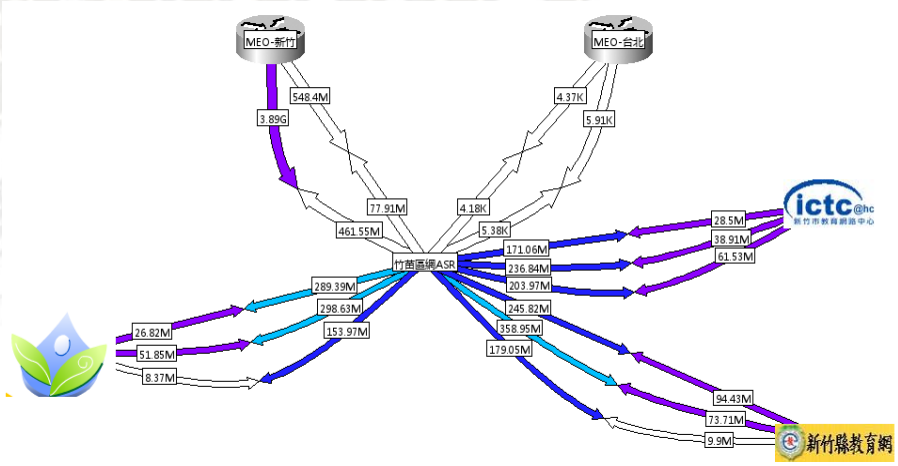
推動網路資訊應用環境之導入情形1

- CACTI監控系統

(範例:竹苗區域網路中心即時流量圖)

http://cacti.hcrc.edu.tw/cacti/plugins/weathermap/weathermap-cacti-plugin.php





推動網路資訊應用環境之導入情形2

- IPV6位址分配表

大專院校		
單位名稱	IPv6位址	狀態
交通大學	2001:288:4001::/48	已設定
聯合大學	2001:288:4002::/48	已設定
新竹教育大學	2001:288:4003::/48	已設定
中華大學	2001:288:4004::/48	已設定
明新科技大學	2001:288:4005::/48	已設定
玄奘大學	2001:288:4006::/48	已設定
大華技術學院	2001:288:4007::/48	已設定
元培科技大學	2001:288:4008::/48	已設定
育達商業技術學院	2001:288:4009::/48	已設定
亞太創意技術學院	2001:288:400A::/48	已設定
中國科技大學	2001:288:400B::/48	已設定

教育網路中心		
單位名稱	IPv6位址	狀態
新竹市網連線單位	2001:288:4200::/39	已設定
新竹市網	2001:288:4200::/48	
新竹縣網連線單位	2001:288:4400::/39	已設定
新竹縣網	2001:288:4400::/48	
苗栗縣網連線單位	2001:288:4600::/39	已設定
苗栗縣網	2001:288:4600::/48	

推動網路資訊應用環境之導入情形2

- IPV6位址分配表

高中職		
單位名稱	IPv6位址	狀態
新竹高中	2001:288:4010::/48	已設定
新竹高商	2001:288:4016::/48	已設定
曙光女中	2001:288:400F::/48	已設定
實驗高中	2001:288:4015::/48	已設定
新竹高工	2001:288:400D::/48	已設定

其他單位		
單位名稱	IPv6位址	狀態
食品工業發展研究所	2001:288:4018::/48	已設定

推動網路資訊應用環境之導入情形3

- DNS 支援IPv6
  - ✓ 竹苗區域網路中心
  - ✓ 新竹市教育網路中心
  - ✓ 新竹縣教育網路中心
  - ✓ 苗栗縣教育網路中心
  - ✓ 交通大學
  - ✓ 新竹高中
  - ✓ 新竹高商
  - ✓ 曙光女中
- 單位網頁支援IPv6
  - ✓ 竹苗區域網路中心
  - ✓ 新竹市教育網路中心
  - ✓ 新竹縣教育網路中心
  - ✓ 苗栗縣教育網路中心
  - ✓ 交通大學
  - ✓ 新竹高中
  - ✓ 新竹高商
  - ✓ 曙光女中

推動網路資訊應用環境之導入情形4

－網路資訊安全設備

➢ Paloalto L7資訊安全設備

- 本年度自編經費維護區網頻寬管理暨資訊安全設備。
- 將TACERT及Paloalto log 提供之威脅名單設定阻擋機制。
  a. 威脅名單連線至區網連線單位一率阻擋。
  b. 區網連線單位連線至威脅名單一率阻擋

- Qos管理機制
  a. 以國中小、高中、大專院校分別設定使用網路之優先權
  b. 管理時段為：星期一 至 星期五 ，上午 08:00 ~ 16:00
  其餘時段無設定

- 學術網路骨幹100G建設已建置完畢，是否還有需要進行分層式QOS控管機制。

5. 網路應用創新服務情形

- 一般區網網路服務
  - 網域名稱(DNS)相關服務
  - 網頁(WWW/HTTP /Proxy)相關服務
- 特殊服務
  - CACTI監控系統：

    a.提供系統範本(vsphere 版本)下載。

    b.協助竹苗區域網路中心連線單位建置。
  - 校園資訊服務節能計畫
  - 資安防護機制
- 到校服務

網路應用與創新服務(監控系統)

CACTI監控系統—協助竹苗區域網路中心連線單位建置

連結網址：

http://www.hcrc.edu.tw/node/227

本年度已協助建置完成單位
聯合大學
育達科技大學
亞太創意技術學院
新竹實驗高中
新竹高商
曙光女中
新竹縣網路中心
新竹高工

網路應用與創新服務(監控系統)

CACTI監控系統—頻寬滿載提醒

設定警戒值依照各連線單位所申請之頻寬，超過上限90%時系統自動寄出通知信件給單位網管，以達到即時提醒頻寬即將滿載之訊息。

<< Previous | Showing Rows 1 to 13 of 13 [1] | Next >>

Actions	Name	ID	Type	Trigger	Duration	Repeat	Warn Hi/Lo	Alert Hi/Lo	BL Hi/Lo	Current	Triggered**	Enabled
	國立清華大學南大校區-區網-C6K - Traffic - 203.68.12.109 - Gi1/10 [traffic_in]	1	High/Low	*1 Minute*	N/A	Never	900/-	-/0.001	N/A	11.7299	no	Enabled
	國立清華大學南大校區-區網-C6K - Traffic - 203.68.12.109 - Gi1/10 [traffic_out]	2	High/Low	*1 Minute*	N/A	Never	900/-	-/0.001	N/A	106.7379	no	Enabled
	聯合-區網-C6K - Traffic - 203.68.12.81 - Gi1/4 [traffic_in]	3	High/Low	*1 Minute*	N/A	Never	900/-	-/0.001	N/A	19.6029	no	Enabled
	聯合-區網-C6K - Traffic - 203.68.12.81 - Gi1/4 [traffic_out]	4	High/Low	*1 Minute*	N/A	Never	900/-	-/0.001	N/A	229.8822	no	Enabled
	明新v4--區網-C6K - Traffic - 203.68.12.166 - Vl300 [traffic_in]	5	High/Low	*1 Minute*	N/A	Never	990/-	-/0.001	N/A	26.0841	no	Enabled
	新竹高商-區網-C6K - Traffic - 140.113.0.250 - Vl4 [traffic_in]	7	High/Low	*1 Minute*	N/A	Never	900/-	-/0.001	N/A	0.0959	no	Enabled
	明新v4--區網-C6K - Traffic - 203.68.12.166 - Vl300 [traffic_out]	6	High/Low	*1 Minute*	N/A	Never	990/-	-/0.001	N/A	97.4804	no	Enabled
	新竹高商-區網-C6K - Traffic - 140.113.0.250 - Vl4 [traffic_out]	8	High/Low	*1 Minute*	N/A	Never	900/-	-/0.001	N/A	1.2105	no	Enabled
	新竹高中-區網-C6K - Traffic - 140.113.0.246 - Vl3 [traffic_in]	9	High/Low	*1 Minute*	N/A	Never	900/-	-/0.001	N/A	3.022	no	Enabled
	新竹高中-區網-C6K - Traffic - 140.113.0.246 - Vl3 [traffic_out]	10	High/Low	*1 Minute*	N/A	Never	900/-	-/0.001	N/A	8.3892	no	Enabled
	光復中學-區網-C6K - Traffic - 140.113.0.254 - Vl2 [traffic_out]	12	High/Low	*1 Minute*	N/A	Never	900/-	-/0.001	N/A	16.141	no	Enabled
	光復中學-區網-C6K - Traffic - 140.113.0.254 - Vl2 [traffic_in]	11	High/Low	*1 Minute*	N/A	Never	900/-	-/0.001	N/A	4.0301	no	Enabled
	區網防火牆-PA5060 - Total Active Sessions [pan_ses_activ]	13	High/Low	*1 Minute*	N/A	Every 10 Minutes	1000000/-	800000/-	N/A	356502	no	Enabled

網路應用與創新服務(監控系統)

CACTI監控系統—頻寬滿載提醒

範例：頻寬警戒值設定為990Mbits，目前流量為1021.881Mbits，系通將會自動發送下列訊息至單位網管人員。

A warning has been issued that requires your attention.

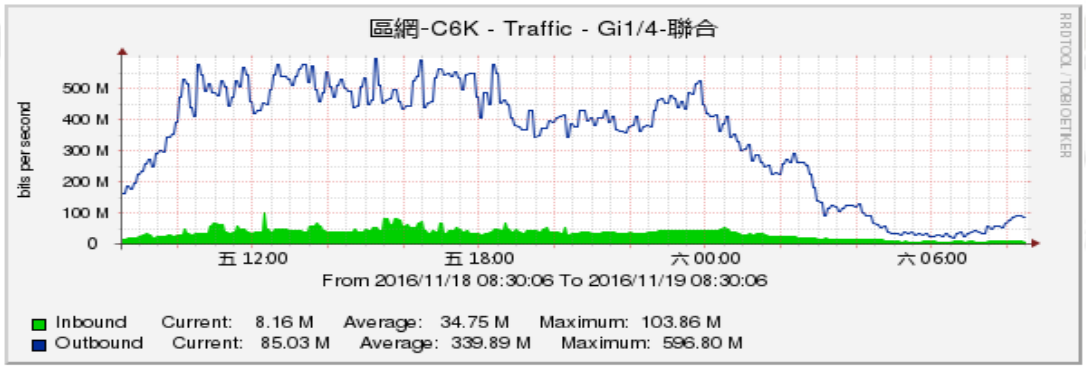
Host: 區網-C6K (192.192.0.113)
URL: http://163.28.64.84/cacti//graph.php?local_graph_id=127&rra_id=1
Message: WARNING: 明新 v4--區網-C6K - Traffic - 203.68.12.166 - Vl300 [traffic_out] [traffic_out] went above threshold of 990 with 1021.881

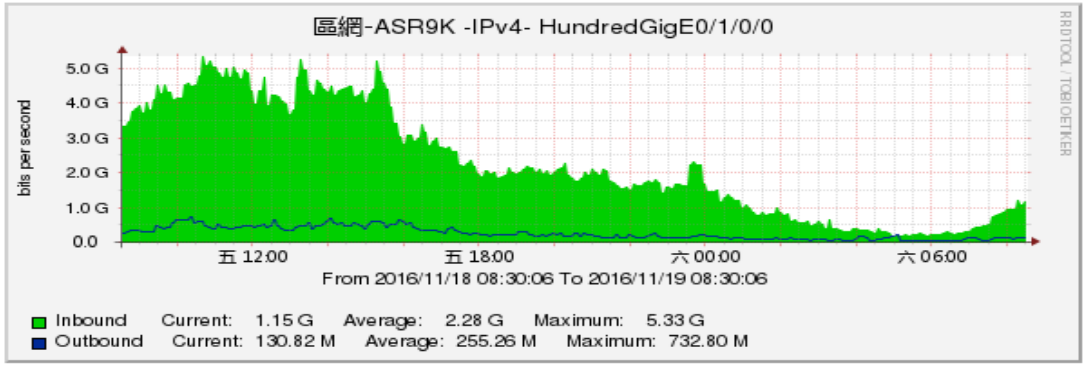
網路應用與創新服務(監控系統)

CACTI監控系統—每日流量使用提醒

範例：各單位獨立設定網路流量圖，於每日上午08:30自動寄信通知單位網管老師前一日網路使用情形。

國立聯合大學





網路應用與創新服務(校園資訊服務節能計畫)

- **計畫簡介：**

1. 營造綠能機房
2. 雲端虛擬化技術將各單位資訊設備集中化管理
3. 提供適當之資通安全防護
4. 改善傳統機房相對耗能以及管理成本偏高等問題
5. 以期更積極地達成兼顧提升服務效能（高穩定度，高效能，高可用性）以及節省能源的多重目標。

網路應用與創新服務(校園資訊服務節能計畫)

- **核心技術：**

1. 利用VMware vSphere做為虛擬平台，具有RAID工能的硬碟儲存櫃做為儲存空間，將原實體機的Server轉換成虛擬機運作於其上
2. 虛擬平台將多台伺服器組成群組，開啟資源共同管理系統與動態電源管理系統，可使用Palo Alto及WAF防火牆系統做安全防護來保護伺服器。
3. 使用Veeam Backup每日做差異性備份。

網路應用與創新服務(校園資訊服務節能計畫)

- **成果效益：**

1. 虛擬化的節能效益推廣至校園以外的範圍，一方面節約能源，另一方面可以提升區域合作對象之資安等級以及提供良好的資訊設備維護。
2. 延續去年與新竹縣市網的合作，加上今年度的推廣，目前本中心提供之服務對象有：新竹高商、新竹市網中心、新竹縣網中心、中華大學、曙光女中、苗栗客庄國小等。

網路應用與創新服務(校園資訊服務節能計畫)

- **已建置之系統收容數：**

  實體主機：29台

總類	數量
節能計畫虛擬主機	144
校建置虛擬主機	537
cPanel帳號收容數	116
總數	797

網路應用與創新服務(資安防護機制)

區網網路資安防護機制

- 目前已於竹苗區網網路使用情形做監控管理。
- 每日將會依據IPS(入侵防禦系統)所統計之報表檢查網路使用情形。
- 當發現異常網路使用之特徵值，將會連絡單位管理人員進行確認。
- 可依單位網管人員確認封鎖IP，待其處理完成後，再解流量封鎖。
- 封鎖類型可分:IP、應用程式、IPS特徵碼或PORT號等等……
- 各單位獨立每日產生TOP 100網路異常流量報表。
- 定期更新TACERT提供之威脅名單，並於資安設備封鎖相關IP。
- 協助各單位升級DNS SERVER

網路應用與創新服務(資安防護機制)

各單位獨立每日產生TOP 100網路異常流量報表

Receive Time	Source address	Destination address	Application	Threat/Content Name	Action
2016/11/19 00:00:42	54.230.141.54	140.126.18.9	web-browsing	Virus/Win32.WGeneric.konuh(2777741)	deny
2016/11/19 00:01:55	220.133.77.137	140.126.17.122	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:02:09	115.159.67.114	140.126.130.229	smtp	MAIL: User Login Brute Force Attempt(40007)	reset-both
2016/11/19 00:02:12	115.159.67.114	140.126.130.229	smtp	MAIL: User Login Brute Force Attempt(40007)	reset-both
2016/11/19 00:02:16	115.159.67.114	140.126.130.229	smtp	MAIL: User Login Brute Force Attempt(40007)	reset-both
2016/11/19 00:02:23	211.72.224.181	140.126.11.251	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:02:31	211.72.224.181	140.126.11.251	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:02:35	61.228.224.235	140.126.12.254	ssh	SSH User Authentication Brute Force Attempt(40015)	reset-both
2016/11/19 00:02:38	211.72.224.181	140.126.11.251	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:02:45	211.72.224.181	140.126.11.251	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:02:52	211.72.224.181	140.126.11.251	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:02:55	94.102.49.193	140.126.15.13	portmapper	UNIX Portmapper Remote Infomation Retrieving Attempt(32796)	reset-server
2016/11/19 00:02:59	211.72.224.181	140.126.11.251	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:03:01	220.133.159.40	140.126.5.155	telnet	Telnet Authentication Brute Force Attempt(40009)	reset-both
2016/11/19 00:03:07	220.133.159.40	140.126.5.155	telnet	Telnet Authentication Brute Force Attempt(40009)	reset-both
2016/11/19 00:03:07	211.72.224.181	140.126.11.251	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:03:10	220.133.159.40	140.126.5.155	telnet	Telnet Authentication Brute Force Attempt(40009)	reset-both
2016/11/19 00:03:14	220.133.159.40	140.126.5.155	telnet	Telnet Authentication Brute Force Attempt(40009)	reset-both
2016/11/19 00:03:14	211.72.224.181	140.126.11.251	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:03:20	115.159.67.114	140.126.130.229	smtp	MAIL: User Login Brute Force Attempt(40007)	reset-both
2016/11/19 00:03:20	220.133.159.40	140.126.5.155	telnet	Telnet Authentication Brute Force Attempt(40009)	reset-both
2016/11/19 00:03:29	115.159.67.114	140.126.130.229	smtp	MAIL: User Login Brute Force Attempt(40007)	reset-both
2016/11/19 00:03:31	211.72.224.181	140.126.11.251	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:04:12	118.163.229.175	140.126.12.254	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:04:13	118.163.229.175	140.126.12.254	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:04:20	61.219.33.102	140.126.7.174	telnet	Telnet Authentication Brute Force Attempt(40009)	reset-both
2016/11/19 00:04:23	61.219.33.102	140.126.7.174	telnet	Telnet Authentication Brute Force Attempt(40009)	reset-both
2016/11/19 00:04:26	61.219.33.102	140.126.7.174	telnet	Telnet Authentication Brute Force Attempt(40009)	reset-both
2016/11/19 00:04:30	61.219.33.102	140.126.7.174	telnet	Telnet Authentication Brute Force Attempt(40009)	reset-both
2016/11/19 00:04:33	61.219.33.102	140.126.7.174	telnet	Telnet Authentication Brute Force Attempt(40009)	reset-both
2016/11/19 00:04:33	220.134.108.59	140.126.11.251	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:04:39	61.219.33.102	140.126.7.174	telnet	Telnet Authentication Brute Force Attempt(40009)	reset-both
2016/11/19 00:04:40	220.134.108.59	140.126.11.251	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:04:43	114.33.29.16	140.126.3.251	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:04:44	218.236.230.113	140.126.147.70	unknown-udp	Win32.Conficker.C p2p(12544)	drop-all-packets
2016/11/19 00:04:48	118.163.239.212	140.126.11.21	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:04:50	114.33.29.16	140.126.3.251	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:04:56	220.134.108.59	140.126.11.251	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:04:56	114.33.29.16	140.126.3.251	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:05:03	114.33.29.16	140.126.3.251	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:05:03	220.134.108.59	140.126.11.251	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:05:09	114.33.29.16	140.126.3.251	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both
2016/11/19 00:05:12	220.134.154.181	140.126.120.62	telnet	Mirai.Gen Command And Control Traffic(13974)	reset-both

網路應用與創新服務(資安防護機制)

定期更新TACERT提供之威脅名單

並於資安設備封鎖相關IP，約匯入850筆

惡意威脅來源清單列表

更新日期：2016年11月16日　　■為本次新增之內容

情資來源：S-ASOC, N-ASOC, A-ISAC　　*本清單為機敏文件，限TANet內部人員使用

清單編號：v2016.45

資料來源	通報時間	IP位置	惡意位址	攻擊型態	國家
S-ASOC	2016/11/12	190.207.71.82		網路攻擊	Venezuela
S-ASOC	2016/11/12	84.204.111.49		網路攻擊	Russian Federation
S-ASOC	2016/11/11	122.131.176.4		網路攻擊	Japan
S-ASOC	2016/11/11	122.131.185.249		網路攻擊	Japan
S-ASOC	2016/11/11	190.203.242.159		網路攻擊	Venezuela
S-ASOC	2016/11/11	221.215.148.30		網路攻擊	China
S-ASOC	2016/11/11	79.111.147.32		網路攻擊	Russian Federation
S-ASOC	2016/11/11	79.129.2.72		網路攻擊	Greece
S-ASOC	2016/11/10	24.31.21.2		網路攻擊	United States
S-ASOC	2016/11/10	121.40.58.212		網路攻擊	China
S-ASOC	2016/11/10	186.92.6.141		網路攻擊	Venezuela
S-ASOC	2016/11/10	186.93.200.141		網路攻擊	Venezuela
S-ASOC	2016/11/10	190.207.91.9		網路攻擊	Venezuela
S-ASOC	2016/11/10	190.78.59.225		網路攻擊	Venezuela
S-ASOC	2016/11/10	216.239.187.166		網路攻擊	United States
S-ASOC	2016/11/10	84.204.109.205		網路攻擊	Russian Federation
S-ASOC	2016/11/9	121.231.142.221		網路攻擊	China
S-ASOC	2016/11/9	122.131.168.108		網路攻擊	Japan
S-ASOC	2016/11/9	122.131.170.22		網路攻擊	Japan
S-ASOC	2016/11/9	175.141.251.206		網路攻擊	Malaysia
S-ASOC	2016/11/9	186.88.240.55		網路攻擊	Venezuela
S-ASOC	2016/11/9	190.201.186.86		網路攻擊	Venezuela
S-ASOC	2016/11/9	190.39.85.30		網路攻擊	Venezuela
S-ASOC	2016/11/9	202.109.143.45		網路攻擊	China
S-ASOC	2016/11/9	219.143.133.113		網路攻擊	China
S-ASOC	2016/11/9	46.17.254.39		網路攻擊	Russian Federation
S-ASOC	2016/11/9	79.111.149.218		網路攻擊	Russian Federation

網路應用與創新服務(資安防護機制)

承上，於資訊安全設備中針對惡意威脅清單IP所執行拒絕(deny)之紀錄。

(rule eq 'TANET-Block-List-out-to-in')

Receive Time	Type	From Zone	To Zone	Source	Source Country	Destination	Destination Country	To Port	Application	Action	Rule	Session End Reason	Bytes
11/20 12:08:14	drop	V-Wire-Untrust	V-Wire-Trust	93.174.93.136	SC	140.126.42.180	TW	5050	not-applicable	deny	TANET-Block-List-out-to-in	policy-deny	60
11/20 12:08:14	drop	V-Wire-Untrust	V-Wire-Trust	94.102.49.174	SC	140.126.129.106	TW	8118	not-applicable	deny	TANET-Block-List-out-to-in	policy-deny	60
11/20 12:08:14	drop	V-Wire-Untrust	V-Wire-Trust	94.102.49.174	SC	140.126.128.255	TW	8118	not-applicable	deny	TANET-Block-List-out-to-in	policy-deny	60
11/20 12:08:14	drop	V-Wire-Untrust	V-Wire-Trust	94.102.49.174	SC	140.126.128.233	TW	8118	not-applicable	deny	TANET-Block-List-out-to-in	policy-deny	60
11/20 12:08:14	drop	V-Wire-Untrust	V-Wire-Trust	94.102.49.174	SC	140.126.134.64	TW	8081	not-applicable	deny	TANET-Block-List-out-to-in	policy-deny	60
11/20 12:08:14	drop	V-Wire-Untrust	V-Wire-Trust	94.102.49.174	SC	140.126.134.49	TW	8081	not-applicable	deny	TANET-Block-List-out-to-in	policy-deny	60
11/20 12:08:14	drop	V-Wire-Untrust	V-Wire-Trust	94.102.49.174	SC	140.126.218.226	TW	8081	not-applicable	deny	TANET-Block-List-out-to-in	policy-deny	60
11/20 12:08:14	drop	V-Wire-Untrust	V-Wire-Trust	106.184.1.178	JP	140.126.73.96	TW	111	not-applicable	deny	TANET-Block-List-out-to-in	policy-deny	60
11/20 12:08:13	drop	V-Wire-Untrust	V-Wire-Trust	93.174.93.136	SC	140.126.133.12	TW	8894	not-applicable	deny	TANET-Block-List-out-to-in	policy-deny	60
11/20 12:08:13	drop	V-Wire-Untrust	V-Wire-Trust	93.174.93.136	SC	140.126.135.102	TW	1028	not-applicable	deny	TANET-Block-List-out-to-in	policy-deny	60
11/20 12:08:13	drop	V-Wire-Untrust	V-Wire-Trust	93.174.93.136	SC	140.126.128.207	TW	5555	not-applicable	deny	TANET-Block-List-out-to-in	policy-deny	60
11/20 12:08:13	drop	V-Wire-Untrust	V-Wire-Trust	94.102.49.174	SC	140.126.219.6	TW	9797	not-applicable	deny	TANET-Block-List-out-to-in	policy-deny	60
11/20 12:08:13	drop	V-Wire-Untrust	V-Wire-Trust	93.174.93.136	SC	140.126.249.213	TW	8892	not-applicable	deny	TANET-Block-List-out-to-in	policy-deny	60
11/20 12:08:13	drop	V-Wire-Untrust	V-Wire-Trust	93.174.93.136	SC	140.126.102.120	TW	8889	not-applicable	deny	TANET-Block-List-out-to-in	policy-deny	60
11/20 12:08:13	drop	V-Wire-Untrust	V-Wire-Trust	93.174.93.136	SC	140.126.98.183	TW	8889	not-applicable	deny	TANET-Block-List-out-to-in	policy-deny	60
11/20 12:08:13	drop	V-Wire-Untrust	V-Wire-Trust	93.174.93.136	SC	140.126.46.21	TW	9000	not-applicable	deny	TANET-Block-List-out-to-in	policy-deny	60
11/20 12:08:13	drop	V-Wire-Untrust	V-Wire-Trust	93.174.93.136	SC	140.126.67.70	TW	8089	not-applicable	deny	TANET-Block-List-out-to-in	policy-deny	60
11/20 12:08:13	drop	V-Wire-Untrust	V-Wire-Trust	93.174.93.136	SC	140.126.13.181	TW	8889	not-applicable	deny	TANET-Block-List-out-to-in	policy-deny	60
11/20 12:08:13	drop	V-Wire-Untrust	V-Wire-Trust	93.174.93.136	SC	140.126.14.105	TW	8889	not-applicable	deny	TANET-Block-List-out-to-in	policy-deny	60
11/20 12:08:13	drop	V-Wire-Untrust	V-Wire-Trust	94.102.49.174	SC	140.126.245.139	TW	8081	not-applicable	deny	TANET-Block-List-out-to-in	policy-deny	60

網路應用與創新服務(資安防護機制)

協助各單位升級DNS SERVER

1. 104年11月20日舉辦「DNS備份及更新」課程
   課程網址 ： http://www.hcrc.edu.tw/node/244
2. 105年10月28日舉辦「 DNS進階管理與除錯」課程
   課程網址 ： http://www.hcrc.edu.tw/node/261
   並附上操作錄影檔提供參考。
3. 提供免費網路空間建立各單位DNS SERVER。
4. 本年度已提供新竹高商一套正版windows2012系統，協助將舊系統windows2003 dns server移轉至新系統，並加強DNS安全性。
5. 106年已排定協助建置單位 ： 新竹高工及曙光女中。

竹苗區網到校服務

- 提供連線單位設備採購驗收注意事項。
  - **本年度協助單位:**

1. 新竹縣網中心：

核心路由器採購建置，由高組長親自與設備商協調及規劃，並於驗收期間提供本校設備驗收範本於新竹縣網中心使用。

2.新竹高工：

全校網路設備及線路更新案，協助規劃及建議網路架構，並與得標廠商討論施做內容，及啟用IPv6網路環境。

3.曙光女中：

校內防火牆更新案，協助查驗防火牆移轉規則，並提供相關建置經驗參考。

校園無線網路系統整合。

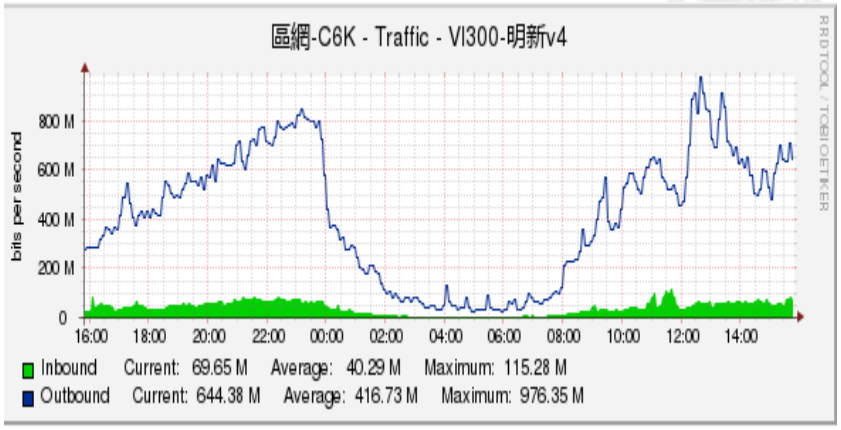
竹苗區網到校服務

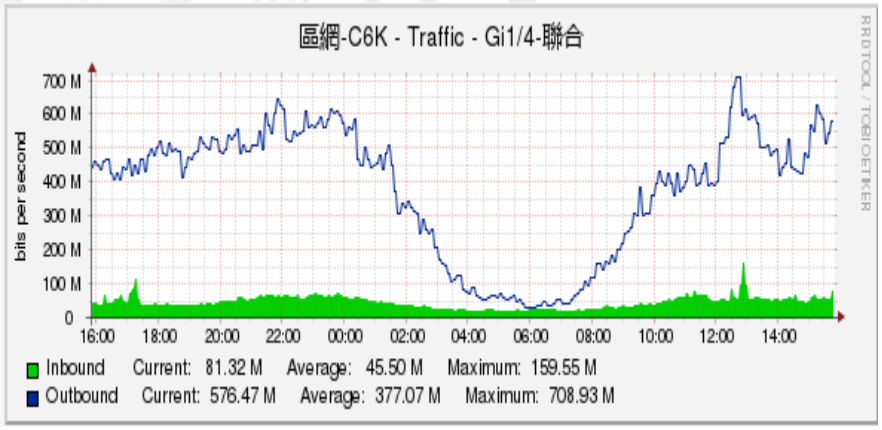
- 設置Tanet Roaming 無線網路環境。

1. 協助連線單位與漫遊認證交換中心處理申請加入相關事項。
2. 提供虛擬機建立Radius認證伺服器，設定VPN連結至漫遊認證交換中心進行伺服器連結。
3. 於本校利用連線單位內帳號密碼使用本校TanetRoaming無線網路漫遊測試。
4. 至連線單位內，利用單位內既有無線網路環境開通TanetRoamin SSID無線網路提供使用。
5. 本年度已協助新竹高商及曙光女中建置完成。

轄下連線單位1G頻寬線路使用調查

- 目前轄下與ISP承租頻寬1G之連線單位共3所，分別為國立清華大學南區分校(原新竹教育大學)、國立聯合大學及明新科技大學。
- 網路服務均僅提供校內使用，包含行政、教學及宿舍網路。
- 經網路流量圖查看，目前網路使用量常期會超過800M以上為國立聯合大學及明新科技大學，期間座落在20:00~02:00，為宿舍網路之使用量居多。





6. 辦理教育訓練及推廣活動情形

日期	活動名稱
105年1月	網管系統建置與設定(in 新竹縣網中心)
105年05月24日	Routing 及 Switch 基礎技術訓練
105年08月04日	DDoS 攻擊的防禦與分析
105年08月27日	OSPF路由協定說明與實作
105年10月28日	DNS進階管理與除錯
105年10月28日	教育部資安通報平台—資安事件鑑識分析與應用

6. 辦理教育訓練及推廣活動情形

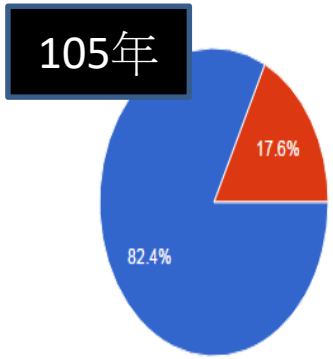
日期	會議	議題
105年05月28日	竹苗區網第一次管委會	1. 學術網路骨幹升級100G專案 A .網路架構說明 B .基礎建設建置規劃 C .移轉時程及注意事項
105年08月10日	竹苗區網第二次管委會	1.竹苗區網中心(交大資訊中心) 雲端節能服務 2.學術網路骨幹升級100G 第二階段時程規劃及說明

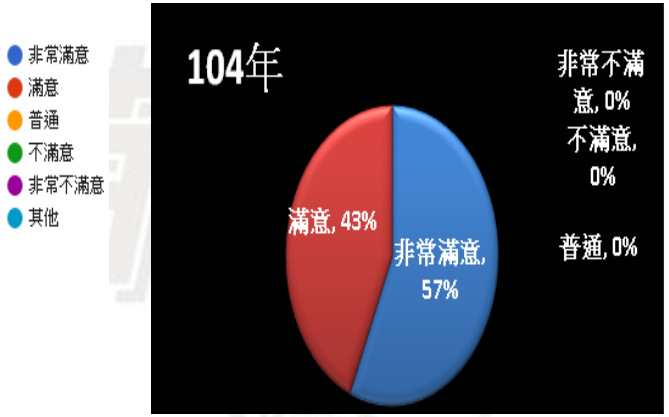
7. 年度計畫所提績效指標辦理情形

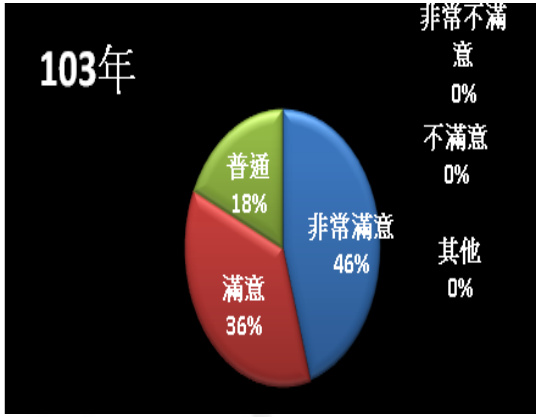
項目	進度
竹苗區域網路中心於2016年7月前重新驗證ISMS	本年度4月28日完成年度正評登錄
協助至少兩所連線學校導入自由軟體CACTI監控系統	新竹縣網中心 新竹高工
協助連線學校教職員參與資安或網路技術教育訓練至少200人次。	已超過200人次
協助至少一所連線學校進行網站弱點掃描、健檢等資安服務。	已有29所連線學校進行網站弱點掃描
協助至少兩所連線單位導入IPv6功能。	新竹高工 食品工業發展研究所

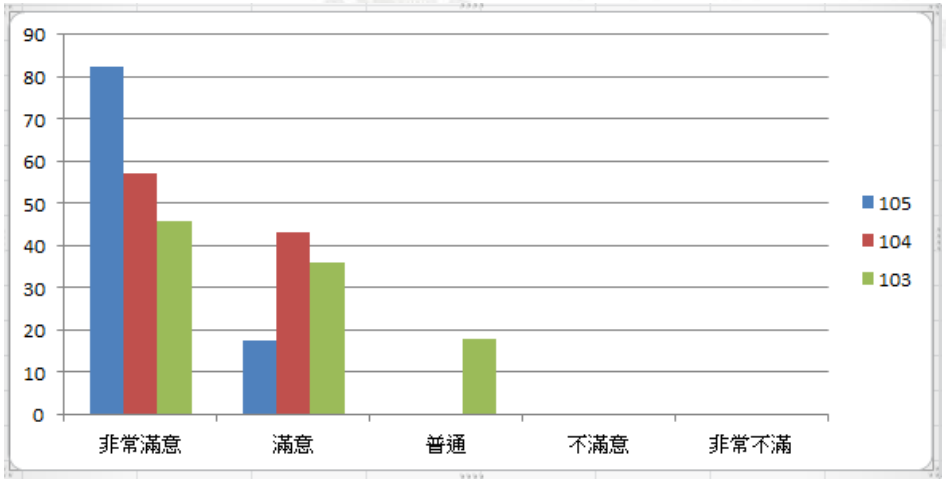
7. 年度計畫所提績效指標辦理情形

105年連線單位針對竹苗區網整體表現滿意度調查表









8. 經費運用情形

教育部補助經費： 1,344,940 元

- 資安維運人力　80%
- 竹苗區網維運　9.5%
- 竹苗區網教育訓練　10%
- 雜支　0.5%

自籌經費 ： 785,000 元

- 頻寬管理暨資訊安全設備維護 100%

9. 結語與綜合建議

1. DNS SERVER版本更新，經調查目前版本較舊之單位多數為高中職，大專院校因有專屬網管人員，故DNS伺服器較有定期更新及維護。由於高中職網管老師流動率高，目前協助高中職建置時，會先以Windows2012為由先考慮。
2. 資安處理相關時數:

   本年度各單位資安通報演練事項，因未注意截止時間為整備期間，已於第一次資安通報演練期間內要求連線單位更新通訊資訊及變更密碼。

	102年	103年	104年	105年
平均通報時數	3.9	2.7	2.54	2.06
平均審核時數	1.55	1.54	2.78	1.51
平均處理時數	6.52	4.37	3.51	2.73

9. 結語與綜合建議

3. 102年教育部提供協助採購之頻寬管理暨資訊安全設備，由於採購時購買3年保固，已於105年過保，由於過保後，設備無法支援威脅特徵碼及病毒特徵碼更新，將無法防禦未知之DDOS攻擊。

4. 本年度針對區網連線單位網管人員已舉辦12場次(3H/場)，類型包含資訊安全、網路資訊及系統服務課程，參與人數約240位網管人員，106年度將持續舉辦以提升各單位網管人員相關資訊能力。

10.106年度預計推動之重點工作

- 配合網路頻寬分流案，降低網路資安設備分析完整流量所造成的系統負載。
- 建置流量分析系統，提供連線單位查詢其網路使用情況。
- 校園資訊服務節能計畫，提供連線單位免費使用網路空間建置伺服器，以達到節省硬體相關支出。
- 持續推動各單位升級DNS SERVER，防止DNS放大攻擊。
- 持續協助連線單位建置網管監控系統，網管系統將提供虛擬化之模組，減免使用單位建置系統之過程。
- 持續宣導網路智慧財產權並舉辦智慧財產權保護活動。
- 持續推動區網資訊安全管理(ISMS)業務
- 視需求將安排資安、網路相關認證課程。

報告完畢
敬請指教

Thanks!