



## TANET 竹苗區域網路中心 104 年度成效報告



國立交通大學  
National Chiao Tung University

國立交通大學 資訊技術服務中心

(104.12.01)



## 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. 105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](mailto: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](mailto: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](mailto: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](mailto:lovetaouc@nctu.edu.tw)
- 電話：03-5712121#31483
- 手機：0921433247



國立交通大學  
National Chiao Tung University



## 網路中心基本資料及人力運作情形<sub>-cont</sub>

- 本區網中心專職與兼任參與維運所投入人力：9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：7人

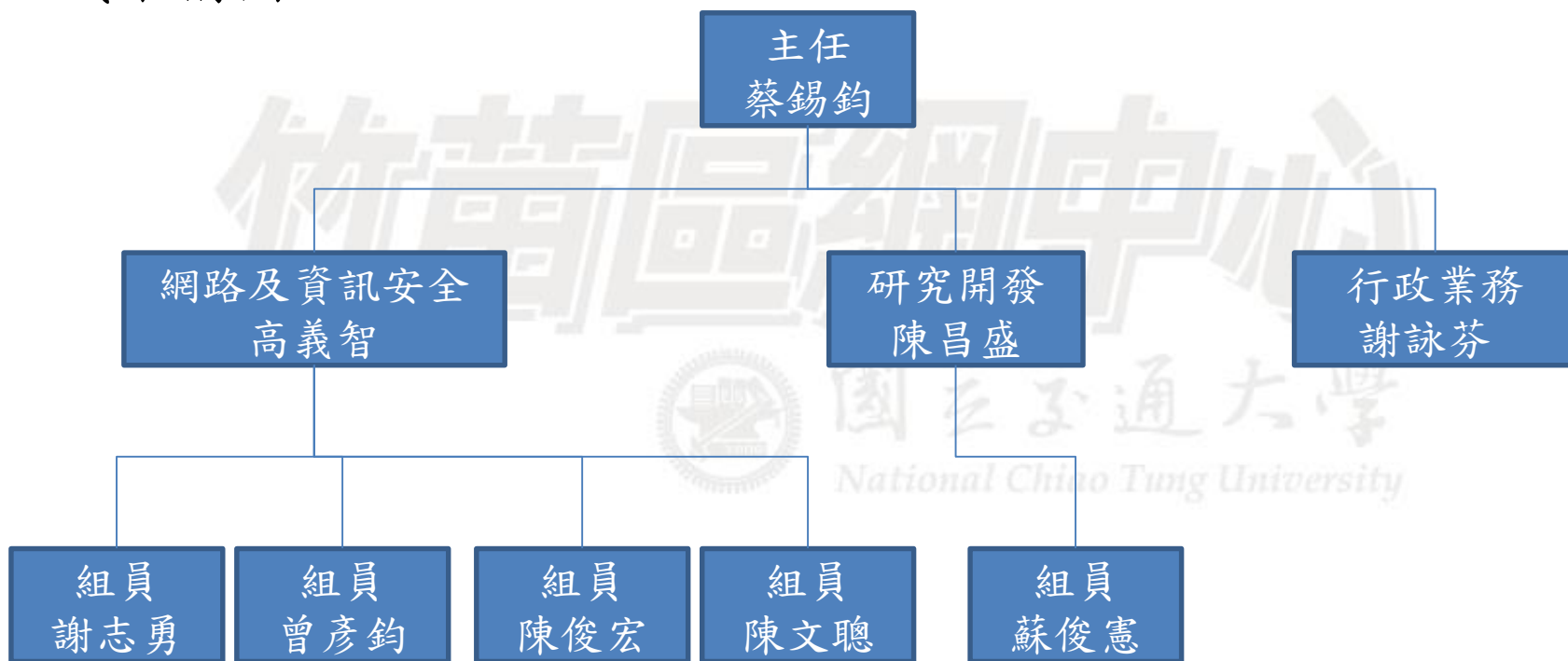


國立交通大學  
National Chiao Tung University



## 網路中心基本資料及人力運作情形<sub>-cont</sub>

### 組織架構圖





## 網路中心基本資料及人力運作情形<sub>-cont</sub>

### 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 | <ol style="list-style-type: none"><li>1.區網網路設備維護設定</li><li>2.建立網路監控系統—cacti<ol style="list-style-type: none"><li>2-1 網路頻寬及時流量圖</li><li>2-2 各單位頻寬超載或過低警告通知</li><li>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</li></ol></li><li>3.協助各單位建立Ipv6網路環境</li><li>4.竹苗區網網頁公告平台建置維護</li><li>5.舉辦連線單位教育訓練課程</li><li>6.協助連線單位設定網路電話</li><li>7.協助連線單位建置單位內網管系統</li><li>8.網路異常處理</li><li>9.輔導所屬連線單位網路維運管理</li></ol> |



## 網路中心基本資料及人力運作情形<sub>-cont</sub>

| 類別   | 姓名  | 工作項目                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 資安人員 | 陳俊宏 | <ol style="list-style-type: none"><li>1. ISO27001教版(ISMS)稽核</li><li>2. 區網資安設備(Paloalto 5060)設定維護<ol style="list-style-type: none"><li>2-1 定期更新並封鎖TACERT提供之威脅名單</li><li>2-2 查看大量異常行為IP並通知單位網管人員</li><li>2-3 提供各單位其資安通報IP之相關流量記錄檔</li><li>2-4 設定調整防火牆規則</li><li>2-5 頻寬使用(QOS)設定整</li></ol></li><li>3. 教育機構防洩漏個資掃描平台維護及審查</li><li>4. 應用程式弱點掃描監測平台維護及審查</li><li>5. 教育部資安通報處理<ol style="list-style-type: none"><li>5-1 竹苗區網中心資安事件處理人員</li><li>5-2 協助連線單位處理資安事件及審核</li><li>5-3 提醒連線單位處理資安事件</li><li>5-4 協助各單位進行教育部資安演練</li></ol></li><li>6. 協助進行營運持續計畫BCP演練</li></ol> |



## 2. 網路中心運作情形

| 業務負責人                                                                                                           | 執掌                                                                                                                                                    | 職務代理人 |
|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| <b>•高義智 組長</b><br><a href="mailto:ykao@mail.nctu.edu.tw">*ykao@mail.nctu.edu.tw</a><br>•03-5731905              | •綜理TANET業務<br>•區網中心業務推動<br>•資安事件協調處理                                                                                                                  | 謝志勇   |
| <b>•陳昌盛 組長</b><br><a href="mailto:cschen@mail.nctu.edu.tw">*cschen@mail.nctu.edu.tw</a><br>•03-5731721          | •TANET業務顧問                                                                                                                                            | 蘇俊憲   |
| <b>•謝志勇</b><br><a href="mailto:shieh0410@mail.nctu.edu.tw">*shieh0410@mail.nctu.edu.tw</a><br>•03-5712121#52823 | 1. 協助TANet區網中心輔導所屬連線單位網路維運管理<br>2. TANET網路骨幹管理      3. TANET路由管理<br>4. ISP介接連線管理      5. 竹苗區網問題諮詢<br>6. 各級學校與機關連線事宜                                   | 曾彥鈞   |
| <b>•曾彥鈞</b><br><a href="mailto:ay529@mail.nctu.edu.tw">*ay529@mail.nctu.edu.tw</a><br>•03-5712121 #52885        | 1. TANET管理委員會      2. TANET教育訓練<br>3. TANET ISMS業務推廣      4. 資通安全宣導服務<br>5. 區網中心網站維護      6. 苗區網問題諮詢<br>7. 竹苗區網網站弱點掃描及防洩漏個資業掃描平台業務<br>8. TANET IPv6推動 | 陳俊宏   |
| <b>•謝詠芬</b><br><a href="mailto:yongfen@mail.nctu.edu.tw">*yongfen@mail.nctu.edu.tw</a><br>•03-5731702           | •處理竹苗區網行政業務                                                                                                                                           | 鄭嘉惠   |
| <b>•蘇俊憲</b><br><a href="mailto:chsu@mail.nctu.edu.tw">*chsu@mail.nctu.edu.tw</a><br>•03-57312121#52808          | 1. TANET IPv6推動      2. VoIP推動<br>3. Mail相關問題諮詢      4. DNS問題諮詢                                                                                       |       |





## 網路中心運作情形<sub>-cont</sub>

- 104年組織運作網址：
- <http://www.hcrc.edu.tw/node/46>

### 104年度執行運作成效

- 基本資料
- 人力狀況
- 組織運作
- 網路架構
- 網路應用與創新服務
- 網路管理工作
- 推廣研習活動
- 經費運用
- 綜合建議

首頁

### 104年度組織運作

- 台灣學術網路竹苗區域網路管理委員會會議記錄：管理委員會會議紀錄
- 連線單位名冊：下載
- 無法連線學校名冊：無
- 參與其他網路合作計畫組織運作機制或內容：  
TANET網路語音交換平台  
TANET無線網路漫遊交換中心



## 網路中心運作情形-cont

- 104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技術小組會議會議紀錄
- 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

### 首頁

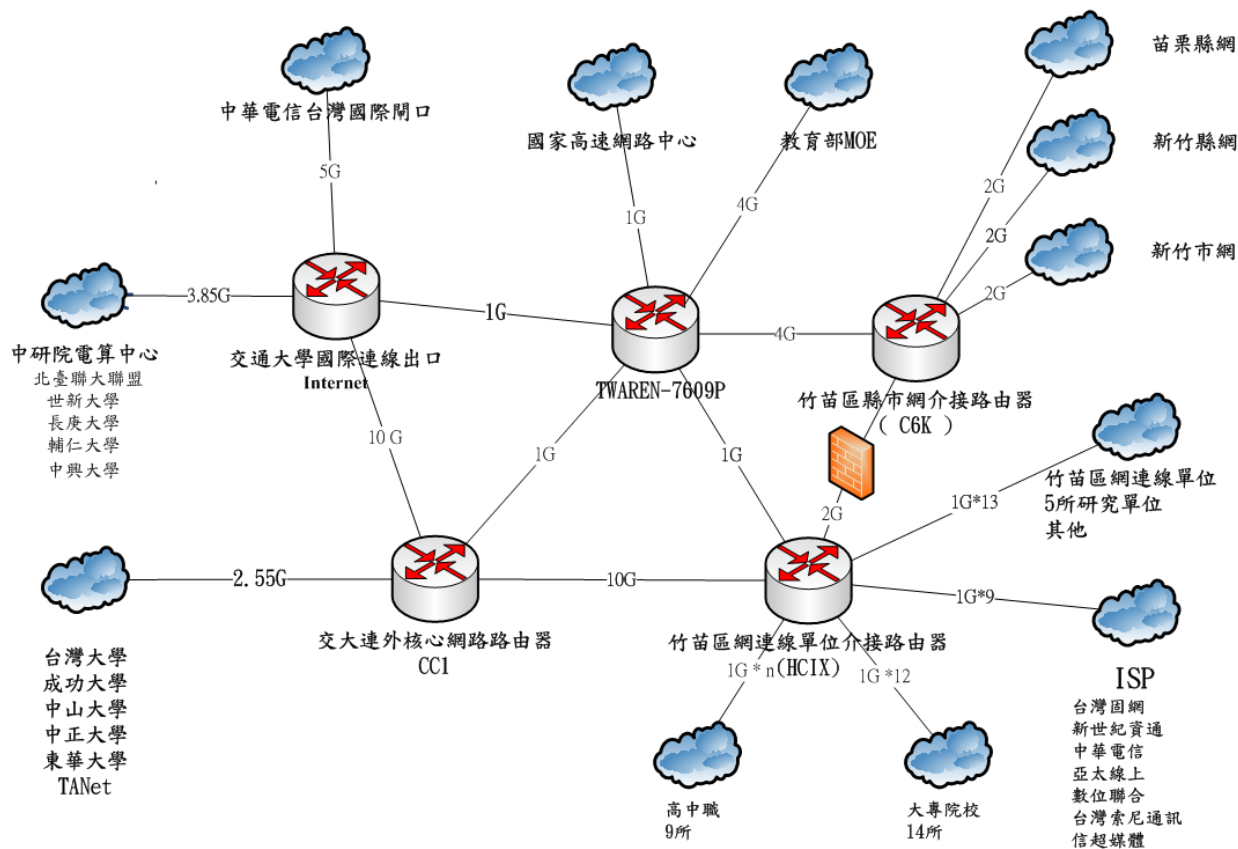
### 會議紀錄

|        |            |            |
|--------|------------|------------|
| 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 |



## 網路中心運作情形-cont

- 104年竹苗區網網路拓撲圖網址：
- <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日完成年度正評登錄

## 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日完成從新授證。





## 資訊安全環境整備<sub>2</sub>-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
- 已掃描成功網站數量：600個網站
- 已上線掃描單位：
  - 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<sub>3</sub>-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：55個單位
- 已掃描成功網站數量：377個網站
- 已上線掃描單位：
- 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
- 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<sub>4</sub>— 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「資通安全及連網人」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://ipr.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

- 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



## – CACTI 監控系統

<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<sub>2</sub>

### － 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<sub>2</sub>

### － 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 |

| 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<sub>3</sub>

- 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<sub>4</sub>

### － 網路資訊安全設備

#### ➤ Paloalto L7 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建設完畢後，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

### ➤ VOIP 分配與使用現況





## 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://163.28.64.198/node/227>

➤ 本年度已協助建置完成之連線單位

- 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



## 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。

| Actions                                                                                                                                                                                                                                                   | Name                           | ID | Type     | Trigger  | Duration | Repeat | Warn Hi/Lo | Alert Hi/Lo | BL Hi/Lo | Current  | Triggered** | Enabled |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|----|----------|----------|----------|--------|------------|-------------|----------|----------|-------------|---------|
|          | 聯合大學 - Gi7/10 [traffic_out]    | 10 | High/Low | 1 Minute | N/A      | Never  | -/0.01     | 900/-       | N/A      | 140.025  | no          | Enabled |
|          | 聯合大學 - Gi7/10 [traffic_in]     | 9  | High/Low | 1 Minute | N/A      | Never  | -/0.01     | 900/-       | N/A      | 21.9412  | no          | Enabled |
|          | 育達科大 - Gi7/1 [traffic_in]      | 7  | High/Low | 1 Minute | N/A      | Never  | -/0.01     | 900/-       | N/A      | 19.6183  | no          | Enabled |
|          | 育達科大 - Gi7/1 [traffic_out]     | 8  | High/Low | 1 Minute | N/A      | Never  | -/0.01     | 900/-       | N/A      | 117.8966 | no          | Enabled |
|    | 明新科大 - Gi7/12 [traffic_in]     | 5  | High/Low | 1 Minute | N/A      | Never  | -/0.01     | 900/-       | N/A      | 20.6509  | no          | Enabled |
|    | 明新科大 - Gi7/12 [traffic_out]    | 6  | High/Low | 1 Minute | N/A      | Never  | -/0.01     | 900/-       | N/A      | 254.9238 | no          | Enabled |
|    | 實驗中學 - VI703 [traffic_in]      | 11 | High/Low | 1 Minute | N/A      | Never  | -/0.01     | 90/-        | N/A      | 6.2034   | no          | Enabled |
|    | 實驗中學 - VI703 [traffic_out]     | 12 | High/Low | 1 Minute | N/A      | Never  | -/0.01     | 90/-        | N/A      | 11.5248  | no          | Enabled |
|    | 亞太創意技術學院 - Gi7/4 [traffic_in]  | 13 | High/Low | 1 Minute | N/A      | Never  | -/0.01     | 400/-       | N/A      | 0.8239   | no          | Enabled |
|    | 亞太創意技術學院 - Gi7/4 [traffic_out] | 14 | High/Low | 1 Minute | N/A      | Never  | -/0.01     | 400/-       | N/A      | 29.2744  | 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200Mbits，目前流量為383.7873Mbits，系統將會自動發送下列訊息至單位網管人員。

ALERT: 明新科大 - Gi7/12 [traffic\_out] [traffic\_out] went above threshold of 200 with 383.7873



竹苗區網通知信

寄給我 ▾



英文 ▾

> 中文(繁體) ▾

翻譯郵件

An Alert has been issued that requires your attention.

**Host:** 竹苗區網\_HCIX (140.113.0.2)

**URL:** [http://163.28.64.111/cacti/graph.php?local\\_graph\\_id=19&rra\\_id=1](http://163.28.64.111/cacti/graph.php?local_graph_id=19&rra_id=1)

**Message:** ALERT: 明新科大 - Gi7/12 [traffic\_out] [traffic\_out] went above threshold of 200 with 383.7873





## 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：

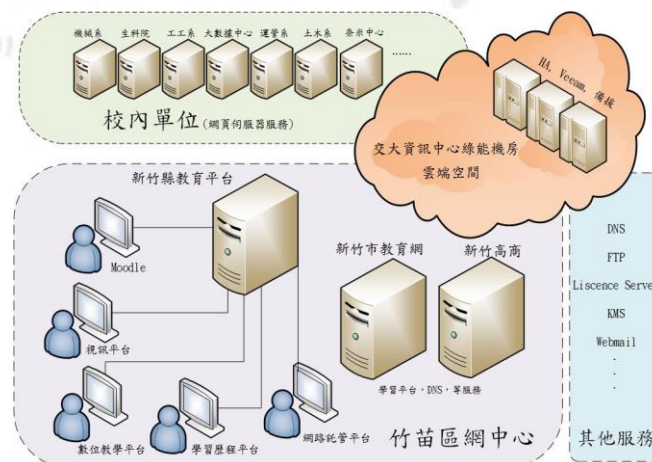
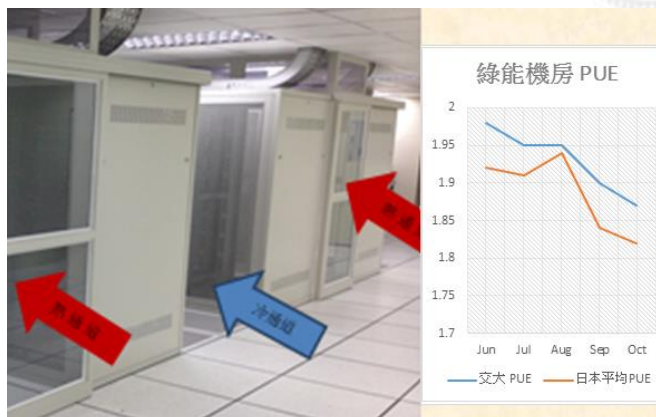
1. 各單位移入的VM已到達65台，每個月可節約5000度電。
2. 新竹縣網之Moodle與教學平台，協同新竹市教育網伺服器及新竹高商部分網頁伺服器已移入綠能機房，同時積極向外推廣校外延伸服務。
3. 集中管理伺服器狀態，達成全天候不停機，同時降低資安風險。
4. 定時自動設定備援檔，提高管理便利性及系統穩定性。
5. 機房伺服器之PUE在VM移入後依然小於標準耗電水平。



## 網路應用與創新服務(校園資訊服務節能計畫)

### • 成果效益 cont :

1. 機房利用冷熱通道大幅度降低冷氣設備用電量，機房PUE僅稍高於日本25大企業平均值。
2. 除了本校內單位各種服務，持續開放校外單位申請進駐。
3. 協助各連線單位建置DNS (bind9.9以上)於此計畫內。

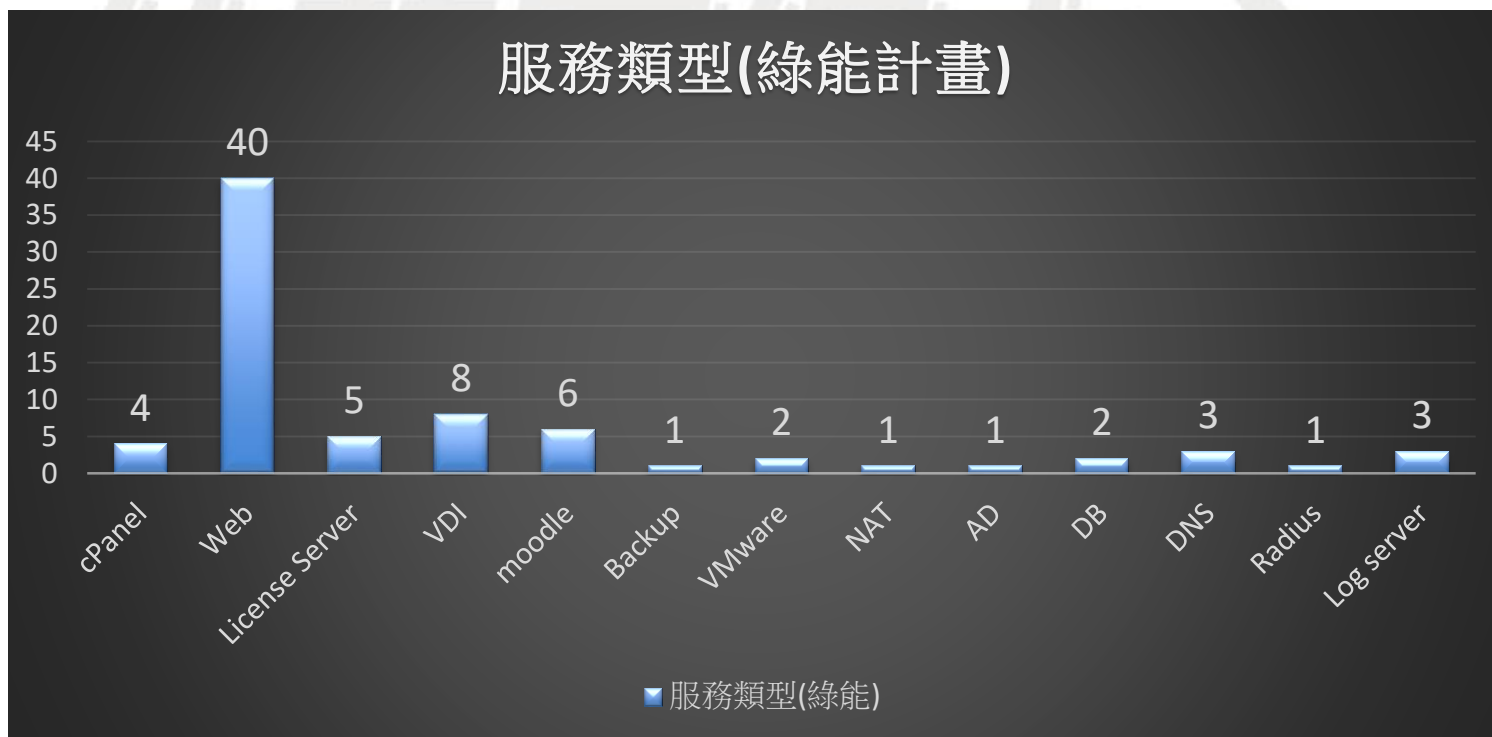






## 網路應用與創新服務(校園資訊服務節能計畫)

- 已建置之服務類別：





## 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

PA-5060 : Wednesday, November 25, 2015

| Source address  | Source Host Name                                      | Destination address | Destination Host Name                                   | Application  | Threat/Content Name                        |
|-----------------|-------------------------------------------------------|---------------------|---------------------------------------------------------|--------------|--------------------------------------------|
| 106.38.184.34   | 106.38.184.34                                         | 120.106.222.66      | r22266.m7.nhcue.edu.tw                                  | unknown-tcp  | HTTP Non RFC-Compliant Response Found      |
| 192.237.226.117 | 192.237.226.117                                       | 120.106.220.201     | r220201.m6.nhcue.edu.tw                                 | web-browsing | Suspicious.Gen Command And Control Traffic |
| 120.106.218.214 | r218214.m3.nhcue.edu.tw                               | 64.66.1.212         | ec2-54-66-1-212.ap-northeast-1.compute.amazonaws.com    | web-browsing | HTTP OPTIONS Method                        |
| 96.211.186.171  | hosted-bf.leaseweb.com                                | 120.106.220.98      | r22098.m6.nhcue.edu.tw                                  | web-browsing | Vmprotect User-Agent Traffic               |
| 120.106.219.66  | r21966.m4.nhcue.edu.tw                                | 64.66.1.212         | ec2-54-66-1-212.ap-northeast-1.compute.amazonaws.com    | web-browsing | HTTP OPTIONS Method                        |
| 120.106.221.120 | r221120.m6.nhcue.edu.tw                               | 123.69.63.227       | 123.69.63.227                                           | web-browsing | HTTP OPTIONS Method                        |
| 120.106.219.66  | r21966.m4.nhcue.edu.tw                                | 64.249.1.103        | ec2-54-249-1-103.ap-northeast-1.compute.amazonaws.com   | web-browsing | HTTP OPTIONS Method                        |
| 116.231.216.26  | 116.231.216.26                                        | 120.106.216.186     | r216186.m1.nhcue.edu.tw                                 | unknown-tcp  | HTTP Non RFC-Compliant Response Found      |
| 116.231.216.24  | 116.231.216.24                                        | 120.106.222.92      | r22292.m7.nhcue.edu.tw                                  | unknown-tcp  | HTTP Non RFC-Compliant Response Found      |
| 140.206.143.44  | 140.206.143.44                                        | 120.106.218.86      | r21886.m3.nhcue.edu.tw                                  | web-browsing | Suspicious user-agent strings              |
| 120.106.220.164 | r220164.m6.nhcue.edu.tw                               | 66.111.190.170      | 66.111.190.170                                          | web-browsing | HTTP OPTIONS Method                        |
| 140.206.230.42  | 140.206.230.42                                        | 120.106.218.86      | r21886.m3.nhcue.edu.tw                                  | web-browsing | Suspicious user-agent strings              |
| 120.106.218.214 | r218214.m3.nhcue.edu.tw                               | 64.249.1.103        | ec2-54-249-1-103.ap-northeast-1.compute.amazonaws.com   | web-browsing | HTTP OPTIONS Method                        |
| 116.231.216.26  | 116.231.216.26                                        | 120.106.219.62      | r21962.m4.nhcue.edu.tw                                  | unknown-tcp  | HTTP Non RFC-Compliant Response Found      |
| 62.68.23.121    | ec2-52-68-23-121.ap-northeast-1.compute.amazonaws.com | 120.106.218.86      | r21886.m3.nhcue.edu.tw                                  | web-browsing | Suspicious user-agent strings              |
| 116.231.216.24  | 116.231.216.24                                        | 120.106.221.126     | r221126.m6.nhcue.edu.tw                                 | unknown-tcp  | HTTP Non RFC-Compliant Response Found      |
| 116.231.216.24  | 116.231.216.24                                        | 120.106.223.97      | r22397.m8.nhcue.edu.tw                                  | unknown-tcp  | HTTP Non RFC-Compliant Response Found      |
| 94.207.37.122   | 94.207.37.122                                         | 120.106.218.86      | r21886.m3.nhcue.edu.tw                                  | web-browsing | Suspicious user-agent strings              |
| 120.106.219.28  | r21928.m4.nhcue.edu.tw                                | 64.261.137.108      | ec2-54-261-137-108.ap-southeast-1.compute.amazonaws.com | web-browsing | HTTP OPTIONS Method                        |
| 183.110.166.122 | 183.110.166.122                                       | 120.106.218.86      | r21886.m3.nhcue.edu.tw                                  | web-browsing | Suspicious user-agent strings              |
| 120.106.221.86  | r22186.m6.nhcue.edu.tw                                | 62.24.224.122       | ec2-52-24-224-122.us-west-2.compute.amazonaws.com       | twiich       | HTTP OPTIONS Method                        |
| 106.39.204.77   | 106.39.204.77                                         | 120.106.222.60      | r22260.m7.nhcue.edu.tw                                  | unknown-tcp  | HTTP Non RFC-Compliant Response Found      |
| 134.169.210.112 | unknown.telstraglobal.net                             | 120.106.218.86      | r21886.m3.nhcue.edu.tw                                  | web-browsing | Suspicious user-agent strings              |
| 140.206.134.220 | 140.206.134.220                                       | 120.106.218.86      | r21886.m3.nhcue.edu.tw                                  | web-browsing | Suspicious user-agent strings              |
| 120.106.216.143 | r216143.m1.nhcue.edu.tw                               | 64.249.1.103        | ec2-54-249-1-103.ap-northeast-1.compute.amazonaws.com   | web-browsing | HTTP OPTIONS Method                        |
| 116.231.216.26  | 116.231.216.26                                        | 120.106.216.143     | r216143.m1.nhcue.edu.tw                                 | unknown-tcp  | HTTP Non RFC-Compliant Response Found      |
| 116.231.216.24  | 116.231.216.24                                        | 120.106.216.63      | r21663.m1.nhcue.edu.tw                                  | unknown-tcp  | HTTP Non RFC-Compliant Response Found      |
| 120.106.220.179 | r220179.m6.nhcue.edu.tw                               | 62.24.224.122       | ec2-52-24-224-122.us-west-2.compute.amazonaws.com       | twiich       | HTTP OPTIONS Method                        |
| 120.106.217.174 | r217174.m2.nhcue.edu.tw                               | 146.148.53.27       | 27.53.148.146.bc.googleusercontent.com                  | web-browsing | HTTP OPTIONS Method                        |
| 120.106.223.36  | r22336.m8.nhcue.edu.tw                                | 64.149.86.130       | ec2-54-149-86-130.us-west-2.compute.amazonaws.com       | web-browsing | HTTP OPTIONS Method                        |
| 120.106.220.173 | r220173.m6.nhcue.edu.tw                               | 62.26.206.34        | ec2-52-26-206-34.us-west-2.compute.amazonaws.com        | twiich       | HTTP OPTIONS Method                        |
| 120.106.217.220 | r217220.m2.nhcue.edu.tw                               | 64.66.1.212         | ec2-54-66-1-212.ap-northeast-1.compute.amazonaws.com    | web-browsing | HTTP OPTIONS Method                        |
| 116.231.216.24  | 116.231.216.24                                        | 120.106.216.66      | r21666.m1.nhcue.edu.tw                                  | unknown-tcp  | HTTP Non RFC-Compliant Response Found      |
| 104.18.63.62    | 104.18.63.62                                          | 120.106.222.14      | r22214.m7.nhcue.edu.tw                                  | web-browsing | JavaScript Obfuscation Detected            |
| 120.106.216.62  | r21662.m1.nhcue.edu.tw                                | 64.249.1.103        | ec2-54-249-1-103.ap-northeast-1.compute.amazonaws.com   | web-browsing | HTTP OPTIONS Method                        |
| 120.106.223.61  | r22361.m8.nhcue.edu.tw                                | 62.26.206.34        | ec2-52-26-206-34.us-west-2.compute.amazonaws.com        | twiich       | HTTP OPTIONS Method                        |
| 116.231.216.26  | 116.231.216.26                                        | 120.106.221.126     | r221126.m6.nhcue.edu.tw                                 | unknown-tcp  | HTTP Non RFC-Compliant Response Found      |
| 116.231.216.26  | 116.231.216.26                                        | 120.106.216.66      | r21666.m1.nhcue.edu.tw                                  | unknown-tcp  | HTTP Non RFC-Compliant Response Found      |



## 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1500筆

惡意威脅來源清單列表

更新日期：2015年11月25日

情資來源：S-ASOC, N-ASOC, A-ISAC

清單編號：v104.47

■為本次新增之內容

\*本清單為機敏文件，限TANet內部人員使用

| 資料來源   | 通報時間       | IP位置            | 惡意位址                              | 攻擊型態                      | 國家                 |
|--------|------------|-----------------|-----------------------------------|---------------------------|--------------------|
| N-ASOC | 2015/11/21 | 104.243.21.100  |                                   | PROTOCOL-DNS DNS query a  | United States      |
| N-ASOC | 2015/11/21 | 151.80.18.238   | shserver.avalle.net               | SSL: OpenSSL TLS DTLS He  | Italy              |
| N-ASOC | 2015/11/21 | 93.174.93.6     | lb.79.7a9f.ip4.static.sl-reverse  | PROTOCOL-DNS DNS query a  | Netherlands        |
| N-ASOC | 2015/11/21 | 94.102.52.213   | supv6650.swiftway.net             | PROTOCOL-DNS DNS query a  | Netherlands        |
| N-ASOC | 2015/11/21 | 159.8.93.183    | hosted-by.ecatel.net              | PROTOCOL-DNS DNS query a  | Switzerland        |
| N-ASOC | 2015/11/21 | 173.246.56.23   | host-173-246-56-23.biznesshosting | PROTOCOL-DNS DNS query a  | United States      |
| N-ASOC | 2015/11/21 | 182.16.1.131    |                                   | HTTP: SqlMap SQL Injectio | Hong Kong          |
| N-ASOC | 2015/11/21 | 184.172.196.100 | 64.c4.acb8.ip4.static.sl-reverse  | PROTOCOL-DNS DNS query a  | United States      |
| N-ASOC | 2015/11/21 | 184.172.196.99  | 64.c4.acb8.ip4.static.sl-reverse  | PROTOCOL-DNS DNS query a  | United States      |
| N-ASOC | 2015/11/21 | 185.106.94.18   | 235.ip-158-69-203.net             | PROTOCOL-DNS DNS query a  | Belize             |
| N-ASOC | 2015/11/21 | 61.187.98.90    |                                   | MSSQL: Password Brute Fo  | China              |
| N-ASOC | 2015/11/21 | 85.114.41.173   | 95.db.559e.ip4.static.sl-reverse  | PROTOCOL-DNS DNS query a  | Croatia            |
| S-ASOC | 2015/11/21 | 106.6.58.41     |                                   | 網路攻擊                      | China              |
| S-ASOC | 2015/11/21 | 109.187.37.73   |                                   | 網路攻擊                      | Russian Federation |
| S-ASOC | 2015/11/21 | 128.72.198.75   |                                   | 網路攻擊                      | Russian Federation |
| S-ASOC | 2015/11/21 | 175.23.30.37    |                                   | 網路攻擊                      | China              |
| S-ASOC | 2015/11/21 | 190.153.81.237  |                                   | 網路攻擊                      | Venezuela          |
| S-ASOC | 2015/11/21 | 199.201.123.231 |                                   | 網路攻擊                      | Canada             |
| S-ASOC | 2015/11/21 | 201.216.180.174 |                                   | 網路攻擊                      | Guatemala          |
| S-ASOC | 2015/11/21 | 201.243.144.12  |                                   | 網路攻擊                      | Venezuela          |
| S-ASOC | 2015/11/21 | 217.29.177.211  |                                   | 網路攻擊                      | Russian Federation |



## 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. 10月份調查各單位DNS版本
  - a. bind 9.9 以下約70%
  - b. bind 9.9 以上約10%
  - c. windows2012 以下約20%
2. 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>
3. 提供免費空間建立各單位DNS SERVER於校園資訊服務節能計畫內



## 竹苗區網網路電話現況

- 已申請號碼之單位—16所

- 交通大學、聯合大學、亞太創意技術學院、明新科技大學、中華大學、育達商業科技大學、玄奘大學、新竹教育大學、苗栗農工、大華技術學院、新竹高商、新竹高中、財團法人食品工業發展研究所、世界高中、新竹高工、竹東高中。

- 已互連之單位---8所

- 交通大學、聯合大學、明新科技大學、育達商業科技大學、新竹高工、苗栗農工、亞太創意技術學院(使用30個網路電話門號)、新竹教育大學。



國立交通大學  
National Chiao Tung University





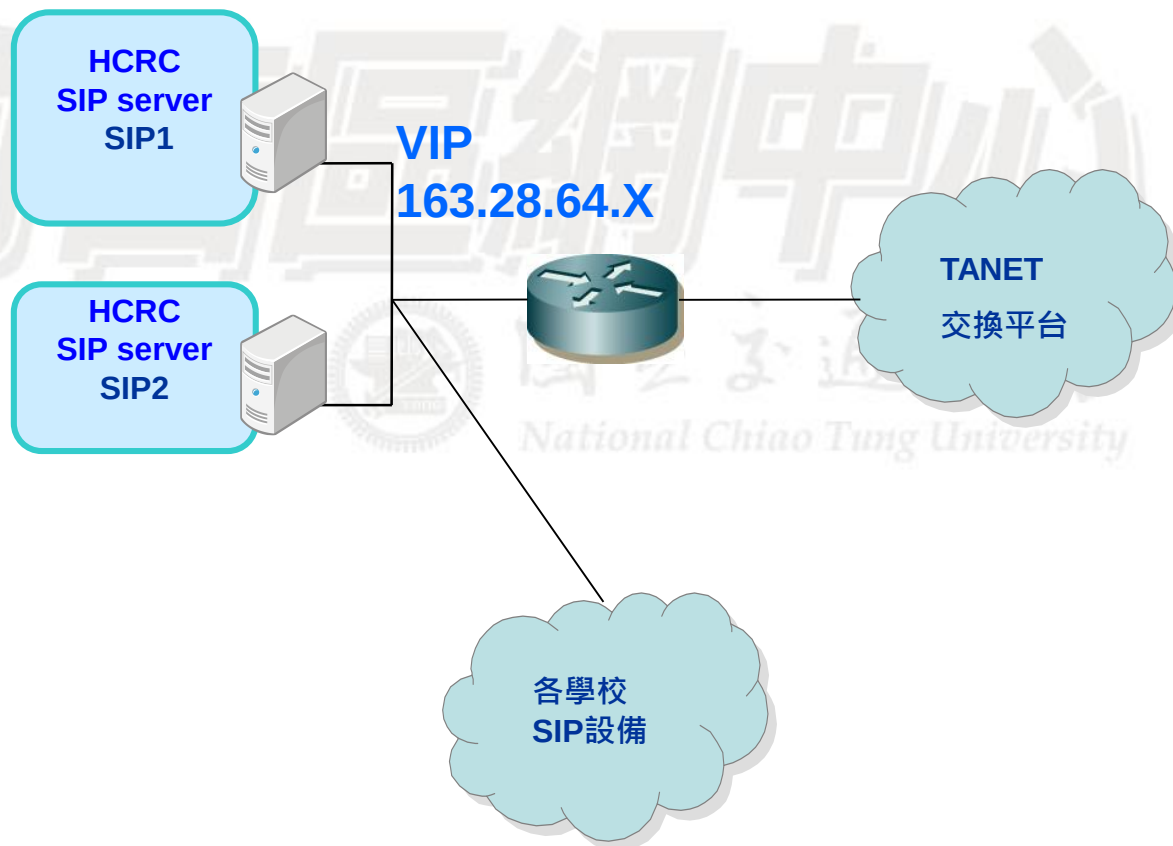
## 竹苗區網網路電話現況





## 竹苗區網網路電話現況(cont.)

- SIP Proxy HA架構圖

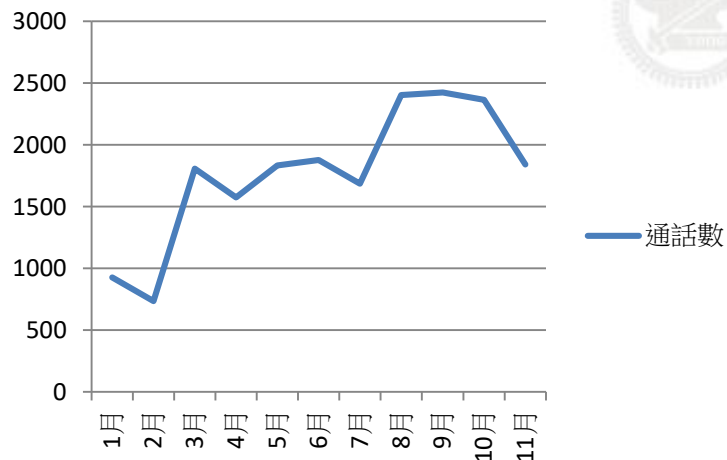




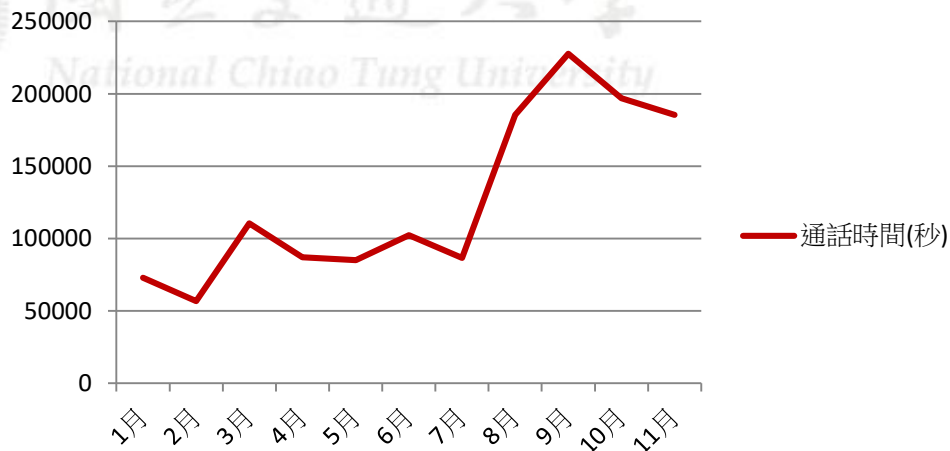
## 竹苗區網網路電話現況(cont.)

- 2015-01~2015-11月之通話數與時間
  - 每月通話數平均1792通，2066分鐘的通話時間

2015/01~2015/11通話數



2015/01~2015/11通話時間





## 6. 辦理教育訓練及推廣活動情形

| 日期           | 活動名稱                                   |
|--------------|----------------------------------------|
| 104年07月15日   | <a href="#"><u>IPV6立即上手及實作</u></a>     |
| 104年08月12日   | <a href="#"><u>網路管理技術課程-DAY1</u></a>   |
| 104年08月13日   | <a href="#"><u>網路管理技術課程-DAY2</u></a>   |
| 104年08月24日   | <a href="#"><u>網路管理技術課程-DAY3</u></a>   |
| 104年08月25日   | <a href="#"><u>網路管理技術課程-DAY4</u></a>   |
| 104年11月20日-上 | <a href="#"><u>校園網路管理應用及安全管理趨勢</u></a> |
| 104年11月20日-下 | <a href="#"><u>DNS備份及版本更新</u></a>      |
| 104年12月08日   | <a href="#"><u>常見的網路攻擊及惡意程式</u></a>    |



## 6. 辦理教育訓練及推廣活動情形

| 日期         | 會議                   | 議題                                                                           |
|------------|----------------------|------------------------------------------------------------------------------|
| 104年07月09日 | 新竹縣(市)網中心與中華電信頻寬討論會議 | 國高中小集縮比<br>頻寬月租費調整                                                           |
| 104年07月15日 | 竹苗區網第一次管委會           | 1. 教育訓練課程意願調查<br>2. 推廣網站應用程式弱點掃描監測平台及防洩漏個資掃描平台<br>3. 推廣校園資訊服務節能計畫            |
| 104年11月20日 | 竹苗區網第二次管委會           | 1. 各單位DNS SERVER版本調查<br>2. 校園資訊服務節能計畫<br>--建置DNS SERVER<br>3. 學術網路100G骨幹升級宣導 |



## 7. 年度計畫所提績效指標辦理情形

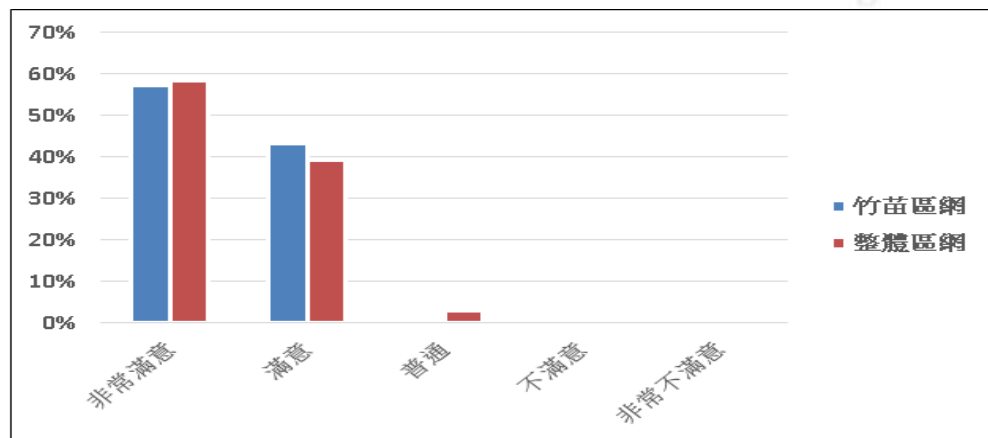
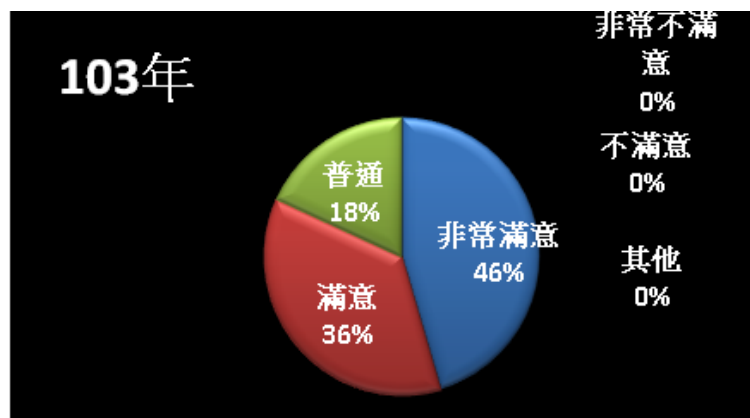
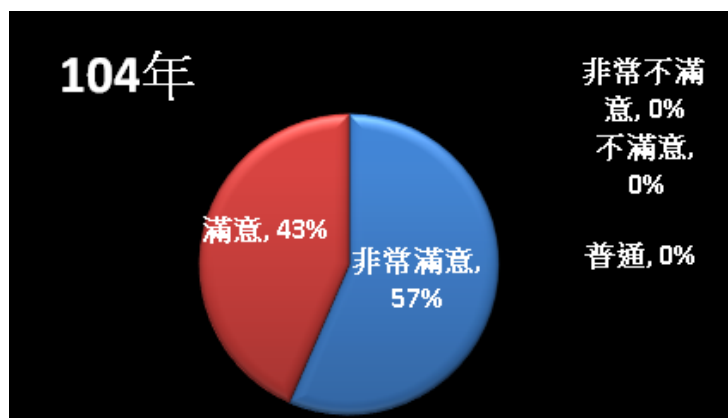
| 項目                             | 進度                          |
|--------------------------------|-----------------------------|
| 竹苗區域網路中心於2015年7月前重新驗證ISMS      | 本年度4月28日完成年度正評登錄            |
| 協助至少兩所連線學校導入自由軟體CACTI監控系統      | 新竹縣網中心<br>國立科學工業園區實驗高級中學    |
| 協助連線學校教職員參與資安或網路技術教育訓練至少200人次。 | 已超過200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。            | 國立科學工業園區實驗高級中學<br>食品工業發展研究所 |





## 7. 年度計畫所提績效指標辦理情形

### 104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：1,345,000 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%



國立交通大學  
National Chiao Tung University



## 9. 結語與綜合建議

1. 已協助3所高中(竹商、曙光及實驗中學)、3所大學(育達、聯合及亞太)及新竹縣網中心建置單位之網管系統-cacti。

2. 資安處理相關時數：

本年度各單位資安處理聯絡人增加至5名，造成單位內無法統一控管聯絡人資訊，若其中一名聯絡人修改”不接收EMAIL或簡訊”將會造成單內所有聯絡人都無法得知有新的資安通報，造成無法及時處理。

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



## 9. 結語與綜合建議

3. 近年來開放大量陸生就讀，陸生所攜帶之資訊設備大多有安裝許多大陸製軟體，例如：360雲盤、百度雲盤等網路空間，造成有開放陸生的大專院校會收到大量的資安通報單，通報有C&C及惡意程式之相關資安事件，擬請資安通報中心對此議題提供處理建議。
4. 本年度針對區網連線單位網管人員已舉辦16場次(3H/場)，類型包含資訊安全、雲端系統服務及系統程式設計課程，參與人數約230位網管人員，105年度將持續舉辦以提升各單位網管人員相關資訊能力。



## 10. 105年度預計推動之重點工作

- 配合「100G骨幹設備採購案」及「100G骨幹線路服務案」提升資訊機房環境設施。
- 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。
- 推動各單位升級DNS SERVER，防止DNS放大攻擊。
- 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。
- 協助各連線單位導入IPv6，高中職連線單位IPv6網路環境推動不易，我們將提供windows server 2012給有意願使用之連線單位試用並協助設定。



## 10. 105年度預計推動之重點工作

- 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。
- SND技術於區網校園網路應用之研究，交通大學將提供有意願之學校每校免費五台AP使用，若必要可於下次技術小組會議簡介。







## 10. 105年度預計推動之重點工作-100G建置案

- 因應「100G骨幹設備採購案」及「100G骨幹線路服務案」
- 本中心已建置3個連續櫃D1、D2及D3櫃，預計放置TWAREN相關網路設備。
- A1櫃預計提供TANET放置相關網路設備。





## 10. 105年度預計推動之重點工作-100G建置案

- 更新機房空調設備
- 建置上吹式20噸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





報告完畢

敬請指教

*Thanks!*