TANET竹苗區域網路中心 107年度成效報告

國立交通大學 資訊技術服務中心
高義智 博士

(107.11.23)

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. 108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

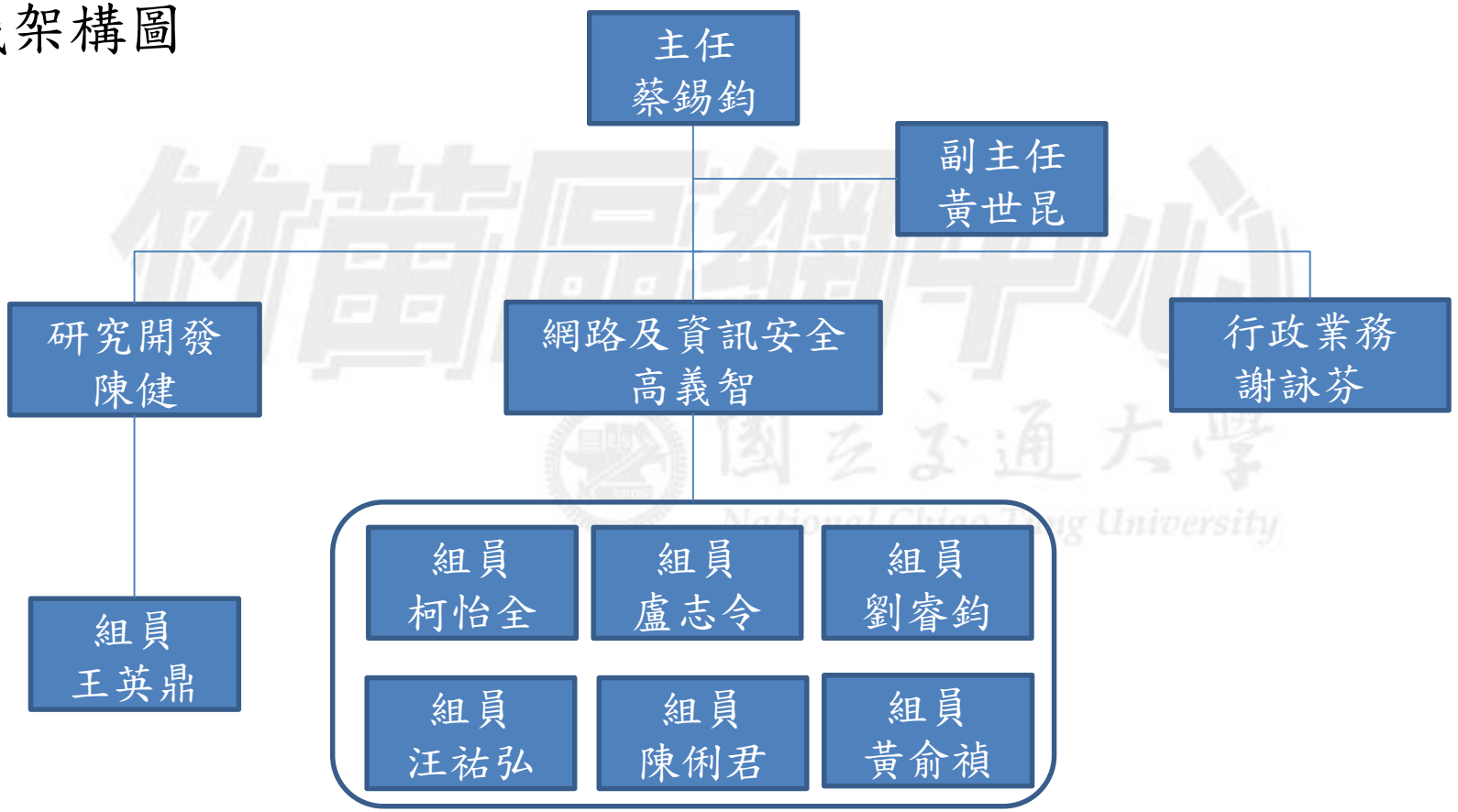
- **單位名稱：竹苗區網中心—國立交通大學**
  - 網址：https://www.hcrc.edu.tw
  - 地址：300新竹市大學路1001號
  - 傳真：03-5714031
- **單位主管：蔡錫鈞 主任**
  - E-mail：sctsai@cs.nctu.edu.tw
  - 電話：03-5731900
- **網路系統組：高義智 組長**
  - E- mail：ykao@mail.nctu.edu.tw
  - 電話：03-5712121#31905
- **網管負責人：柯怡全**
  - E- mail：h0631@nctu.edu.tw
  - 電話：03-5712121#31706
- **資安負責人：汪祐弘**
  - E- mail : youhong@nctu.edu.tw
  - 電話：03-5712121#31483

網路中心基本資料及人力運作情形

- 本區網中心專職與兼任參與維運所投入人力：12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：10人

網路中心基本資料及人力運作情形

組織架構圖



網路中心基本資料及人力運作情形

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	柯怡全	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

類別	姓名	工作項目
資安人員	陳俐君	1.ISO27001教版(ISMS)稽核 2.教育機構防洩漏個資掃描平台維護及審查 3.應用程式弱點掃描監測平台維護及審查 4.教育部資安通報處理 4-1 竹苗區網中心資安事件處理人員 4-2 協助連線單位處理資安事件及審核 4-3 提醒連線單位處理資安事件 4-4 協助各單位進行教育部資安演練 5.協助進行營運持續計畫BCP演練 6. TANET設備資訊機房管理

2. 網路中心運作情形-業務執掌

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	黃世昆 副主任
• 柯怡全 • 0631@nctu.edu.tw • 03-5712121#31706	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	汪祐弘
• 汪祐弘 • youhong@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	柯怡全
• 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	柯怡全
• 謝詠芬 • yongfen@mail.nctu.edu.tw • 03-5731702	•處理竹苗區網行政業務	

網路中心運作情形-組織運作

- 107年組織運作網址 ：
- https://www.hcrc.edu.tw/grade/organize/

107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

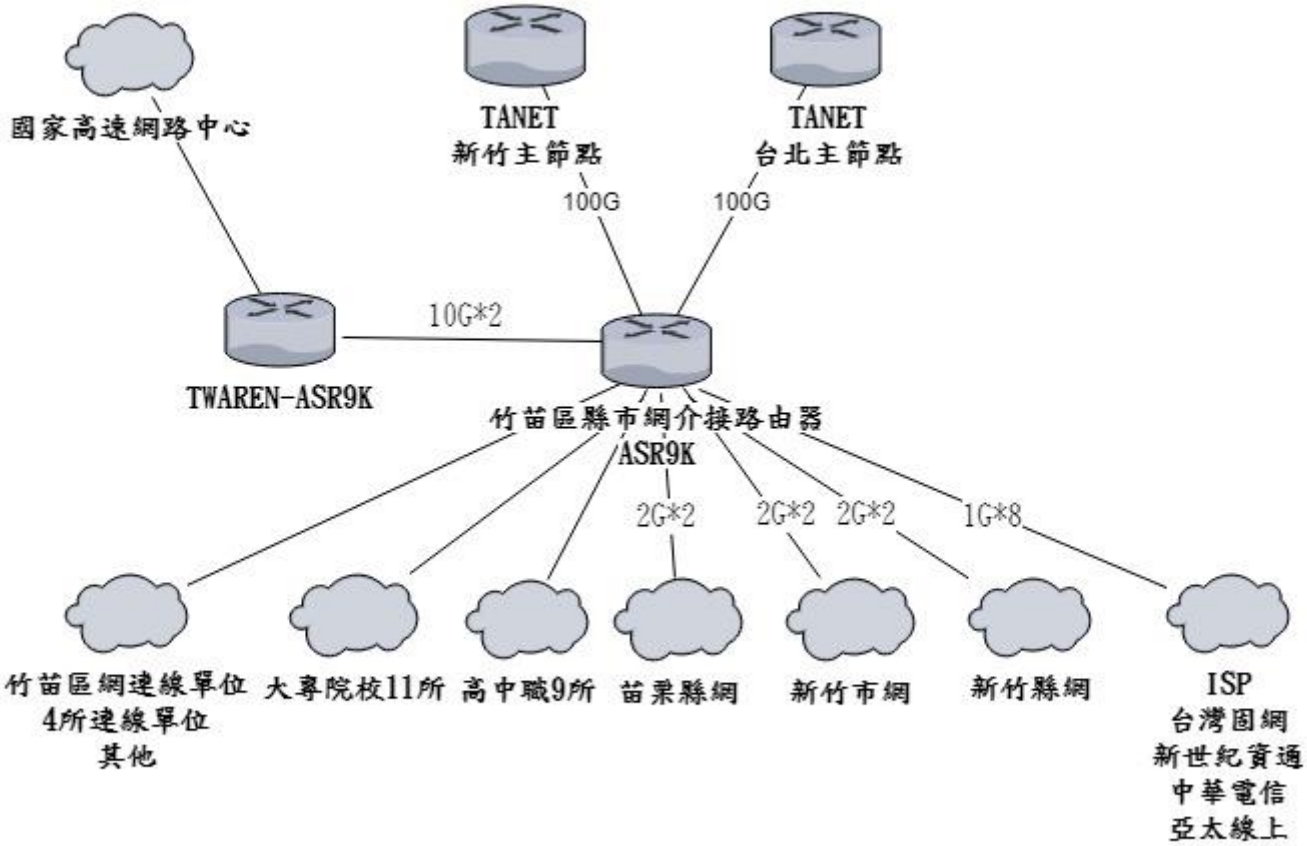
網路中心運作情形-管委會會議記錄

- 107年竹苗區網管理委員會會議紀錄：
- https://www.hcrc.edu.tw/meeting_index/

會議記錄

107學年度	107 學年度第1次會議記錄	107 學年度第2次會議記錄
106學年度	106 學年度第1次會議記錄	106 學年度第2次會議記錄
105學年度	105 學年度第1次會議記錄	105 學年度第2次會議記錄
104學年度	104 學年度第1次會議記錄	104 學年度第2次會議記錄
103學年度	103 學年度第1次會議記錄	103 學年度第2次會議記錄
102學年度	102 學年度第1次會議記錄	102 學年度第2次會議記錄
101學年度	101 學年度第1次會議記錄	
100學年度	100 學年度第1次會議記錄	100 學年度第2次會議記錄

網路中心運作情形-網路拓樸圖



- 107年竹苗區網網路拓墣圖網址：
- https://www.hcrc.edu.tw/structure/

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

◆已於本年度04月26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26日完成複評。

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

No.1001 University Road, Hsinchu City 300, 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, Grading System, and Faculty Email System, provided by the Network System Group, related Technology Development Group, and related Academic Information Group. The scope does not include 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 2.1.

This certificate is valid from 18 June 2018 until 18 June 2021 and remains valid subject to satisfactory surveillance audits.
Re certification audit due before 14 May 2021
Issue 5. Certified since 18 June 2012

Authorised by

SGS United Kingdom Ltd
Rossmore Business Park Ellesmere Port Cheshire CH65 3EN UK
t +44 (0)151 350-6666 f +44 (0)151 350-6600 www.sgs.com

HC SGS 27001 2013 0118

Page 1 of 1

SYSTEM CERTIFICATION ISO/IEC 27001 SGS

UKAS MANAGEMENT SYSTEMS 0005

資訊安全環境整備-竹苗區網網頁弱點掃描

- **連線單位可以透過線上平台進行網站的掃描及排程掃描，並於掃描完成後將掃描結果報告以E-mail方式寄發。**
- **因此平台已不再維護，故已於今年10月關閉，並推動EVS弱掃平台。**
- **相關網址：http://ewavs.hcrc.edu.tw/**
- **已註冊連線人數：53人**
- **已掃瞄成功網站數量：697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、大華科技大學、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。

資訊安全環境整備-教育單位弱點檢測平台

- **連線單位可以透過線上平台進行網站的掃描及排程掃描，並於掃描完成後將掃描結果報告以E-mail方式寄發。**
- **相關網址：https://evs.twisc.ncku.edu.tw/**
- **已掃瞄成功網站數量：5個網站**
- **已上線掃瞄單位：**

  - 大專院校: 交通大學、大華科技大學
  - 高中職 : 光復高中

資訊安全相關服務-竹苗區網防洩漏個資掃描平台

- **連線單位可以透過線上平台進行網站的掃描及排程掃描，並於掃描完成後將掃描結果報告以E-mail方式寄發。**
- **相關網址：https://epdp.hcrc.edu.tw**
- **已註冊連線人數：62個單位**
- **已掃瞄成功網站數量：555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、大華科技大學、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- 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：https://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

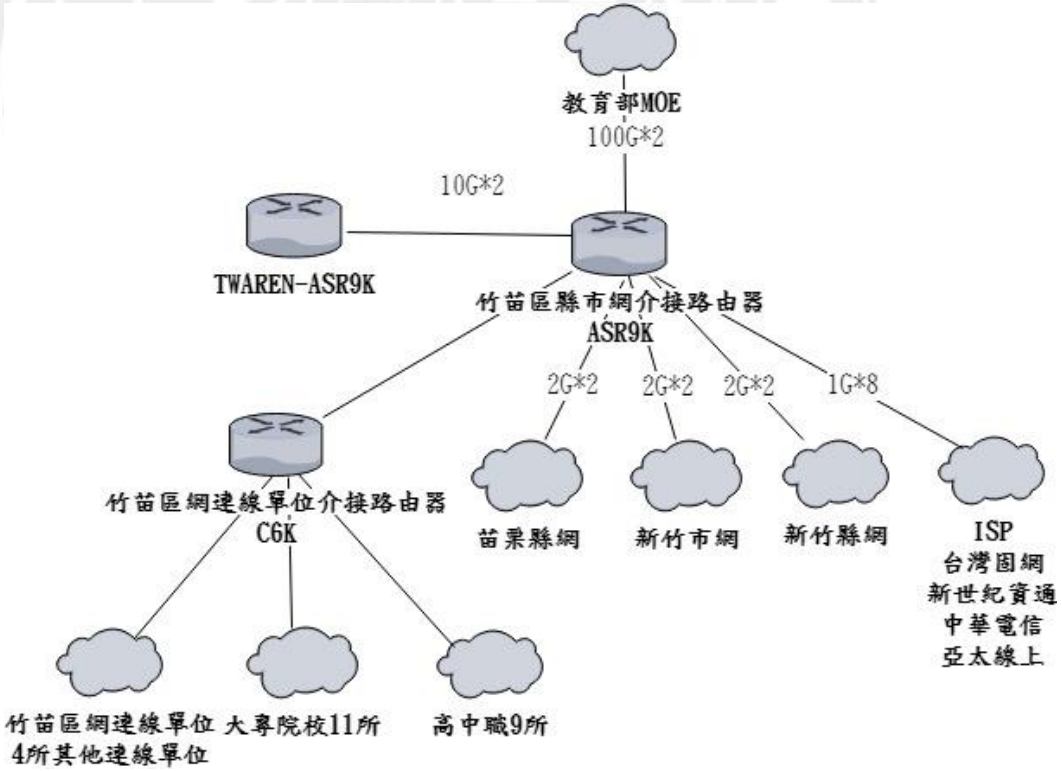
- TANet骨幹設備連線模組升級
- 汰換資訊機房B迴路之老舊UPS
- 建置新版竹苗區網網站
- VoIP使用情形
- 透過CACTI監控系統監控網路流量
- 連線單位導入IPv6
- 網路資訊安全設備

推動網路資訊應用環境之導入情形

– Tanet骨幹設備連線模組升級

舊有架構：

除苗栗縣、新竹縣、新竹市等3縣市網，以及中華電信等ISP線路外，其他連線學校/單位皆經由年限屆退、已無保固之介接路由器C6K連接至TANet。

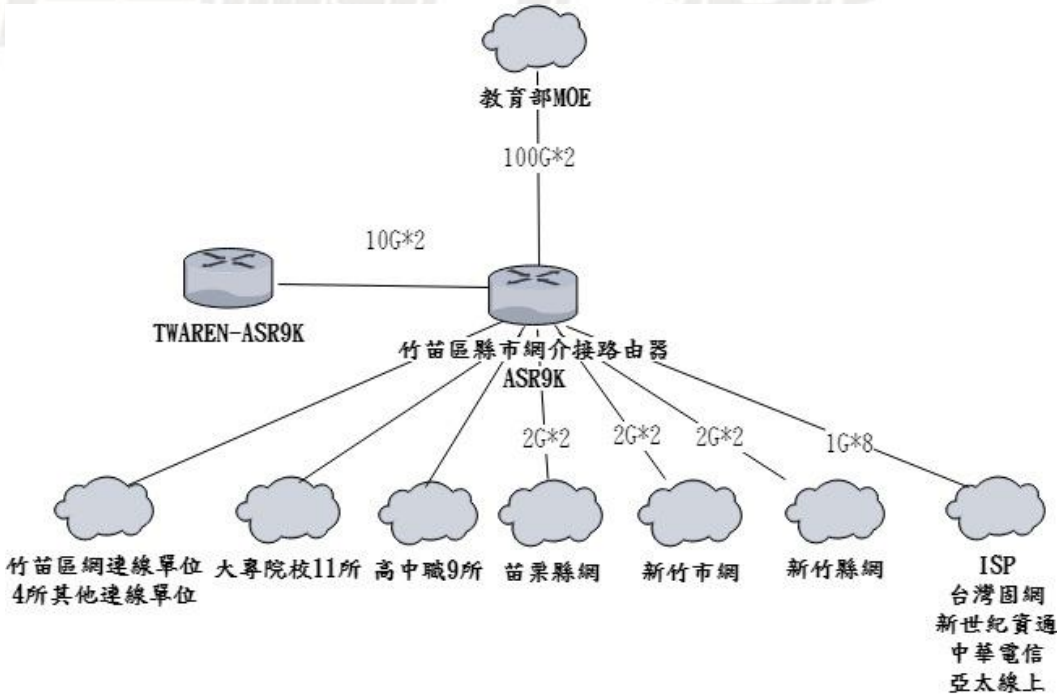


推動網路資訊應用環境之導入情形

– Tanet骨幹設備連線模組升級

升級後架構：

為路由器ASR9K擴充40個1G網路介面，讓路由器ASR9K足以提供所有連線單位使用，而無須另外介接路由器C6K。以此達到簡化架構並完成連線單位統一進線至骨幹網路設備等目的。



推動網路資訊應用環境之導入情形

–汰換資訊機房B迴路之老舊UPS

107年9月完成汰換資訊機房B迴路之老舊UPS，與既有模組式150KVA UPS並聯，減少10%以上電力耗損，增進節能效益。

推動網路資訊應用環境之導入情形

–建置新版竹苗區網網站

- 新版之竹苗區網中心網頁支援https協定，並支援手機版網頁瀏覽功能。

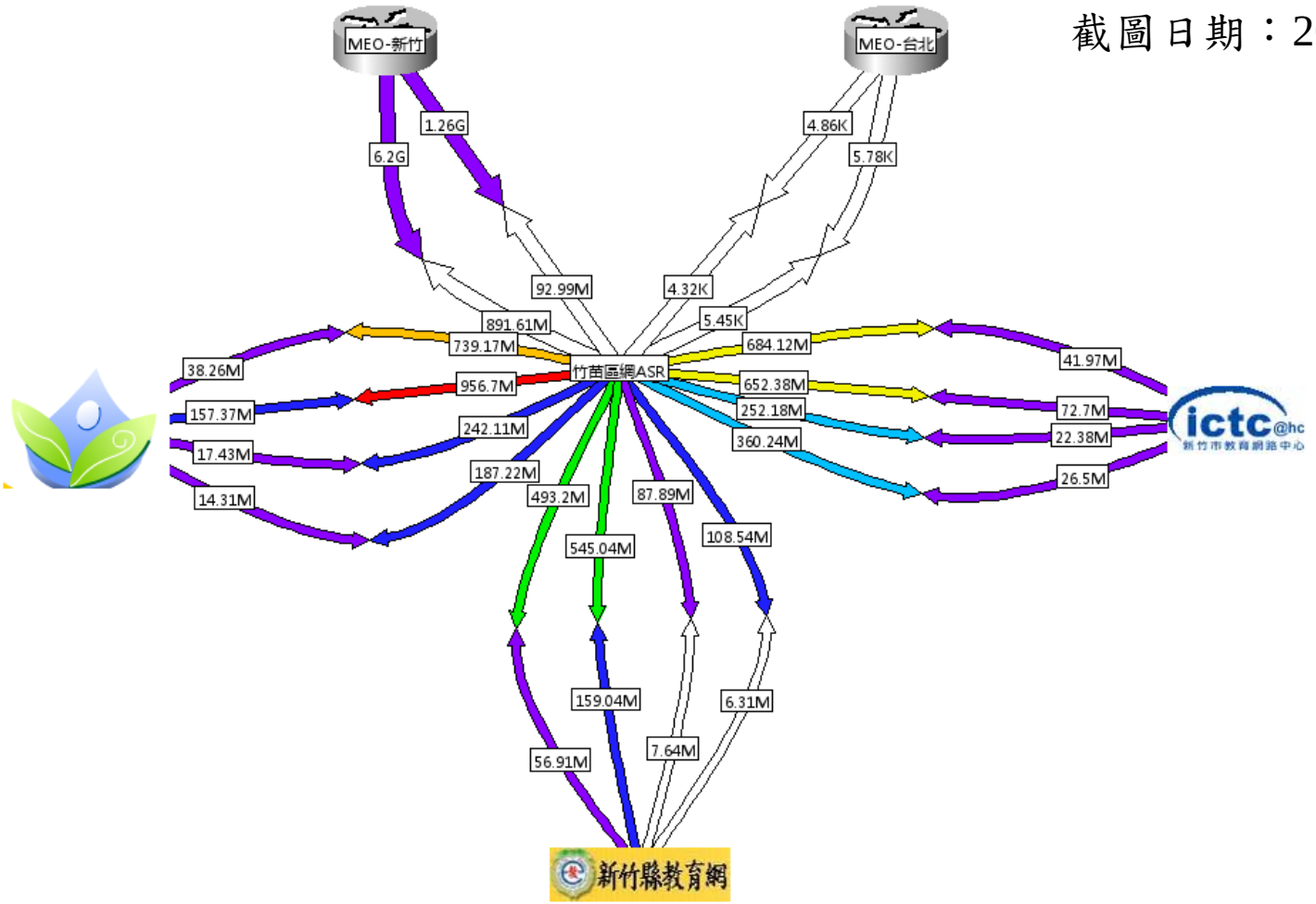
最新消息

2018年10月17日 14:26	【漏洞預警】Juniper NFX系列之Junos OS 18.1版本存在安全漏洞(CVE-2...
2018年10月17日 14:26	【漏洞預警】Juniper Junos OS之NTP套件存在多個安全漏洞，允許攻擊者遠端執行任...
2018年8月28日 14:05	【漏洞預警】Apache Struts 2.3.X與2.5.X系列版本存在允許攻擊者遠端執行任...
2018年8月17日 12:00	【漏洞預警】多款HP噴墨印表機存在安全漏洞(CVE-2018-5924與CVE-2018-59...
2018年5月	【漏洞預警】多款DrayTek路由設備存在零時差漏

推動網路資訊應用環境之導入情形

– CACTI監控系統　(範例:竹苗區域網路中心即時流量圖)

https://www.hcrc.edu.tw/graph/

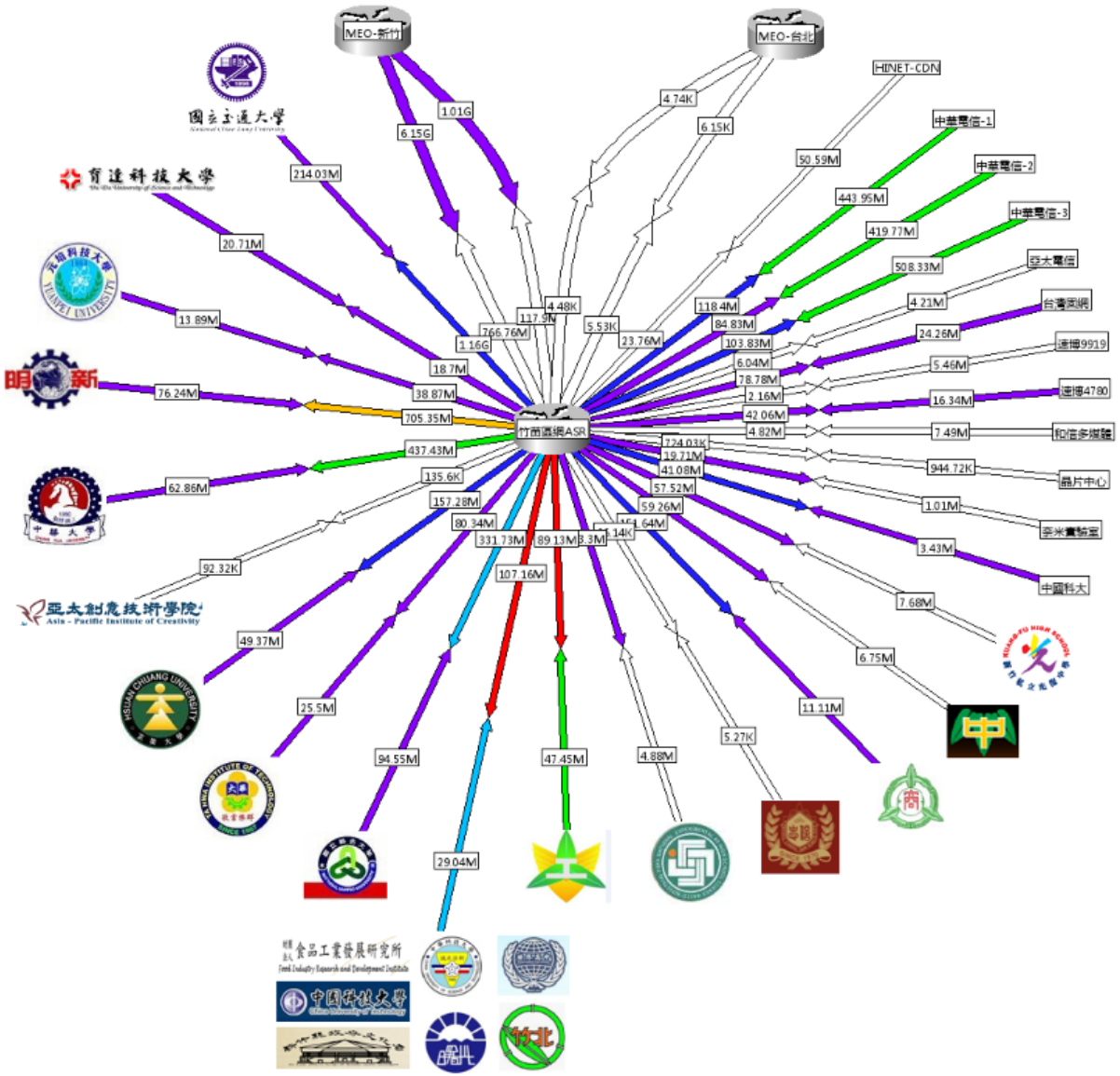


截圖日期：2018/10/30

竹苗區網中心

Created: Oct 30 2018 09:45:04

截圖日期：2018/10/30



推動網路資訊應用環境之導入情形

–連線單位導入IPv6

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
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
大華科技大學	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

–連線單位導入IPv6

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
世界高中	2001:288:4013::/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

–連線單位導入IPv6

- 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
✓ 中華科技大學新竹分校
✓ 元培科技大學
✓ 世界高中

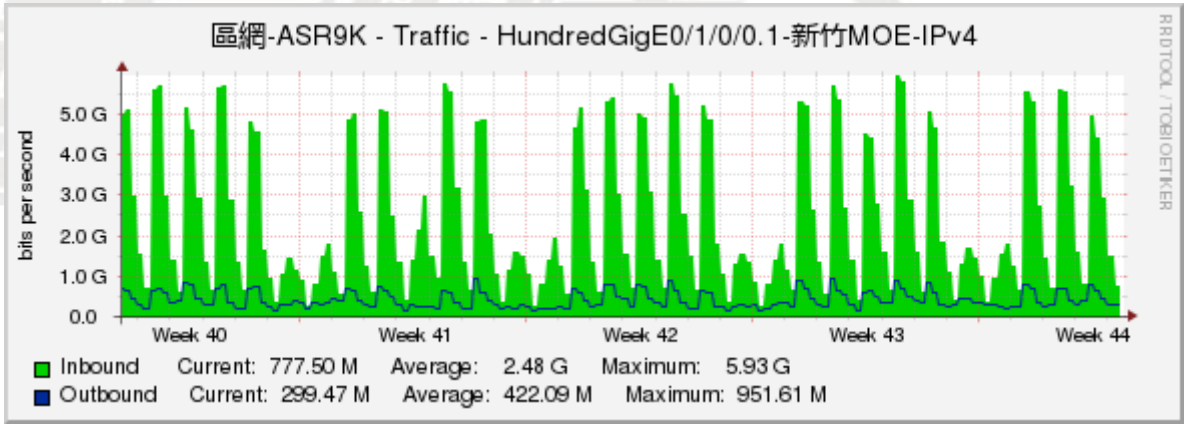
- 單位網頁支援IPv6

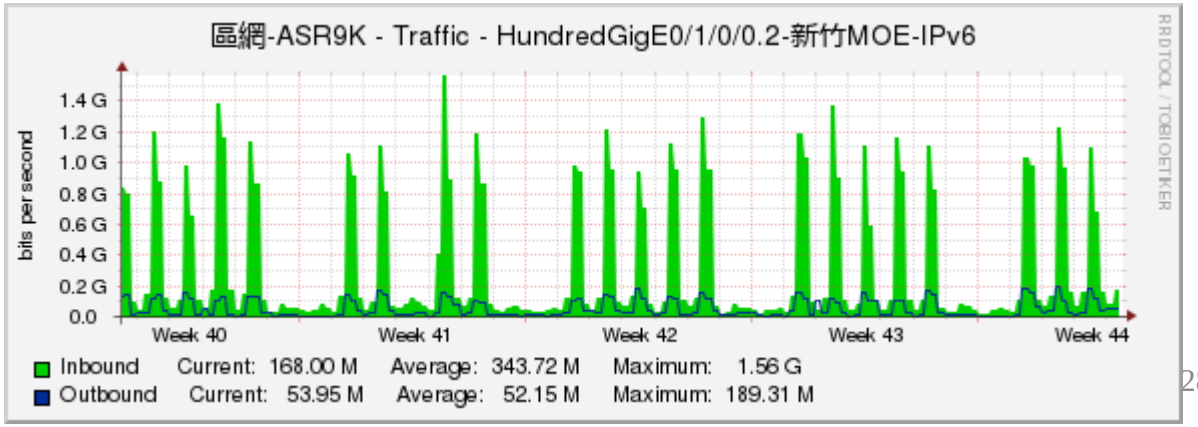
✓ 竹苗區域網路中心
✓ 新竹市教育網路中心
✓ 新竹縣教育網路中心
✓ 苗栗縣教育網路中心
✓ 交通大學
✓ 新竹高中
✓ 新竹高商
✓ 曙光女中
✓ 中華科技大學新竹分校
✓ 元培科技大學
✓ 世界高中

推動網路資訊應用環境之導入情形

–連線單位導入IPv6

- 竹苗區網IPv4、IPv6流量對照圖
- IPv6占總流量約12%



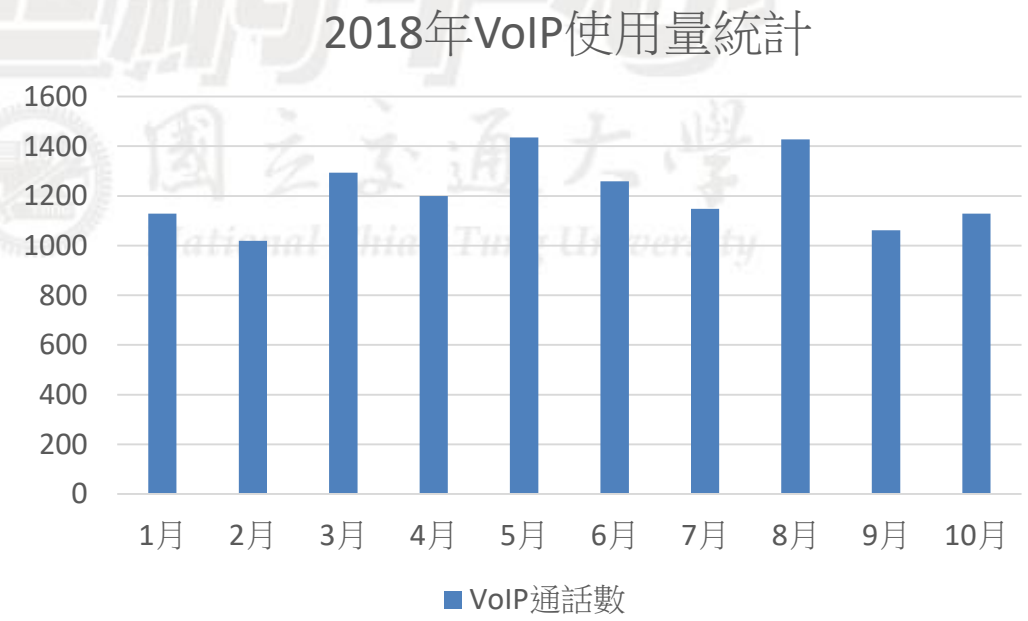


推動網路資訊應用環境之導入情形

–VoIP使用情形

- 竹苗區網SIP連線

✓ MOE
✓ TANET
✓ 玄奘大學
✓ 明新科大
✓ 聯合大學
✓ 苗栗農工

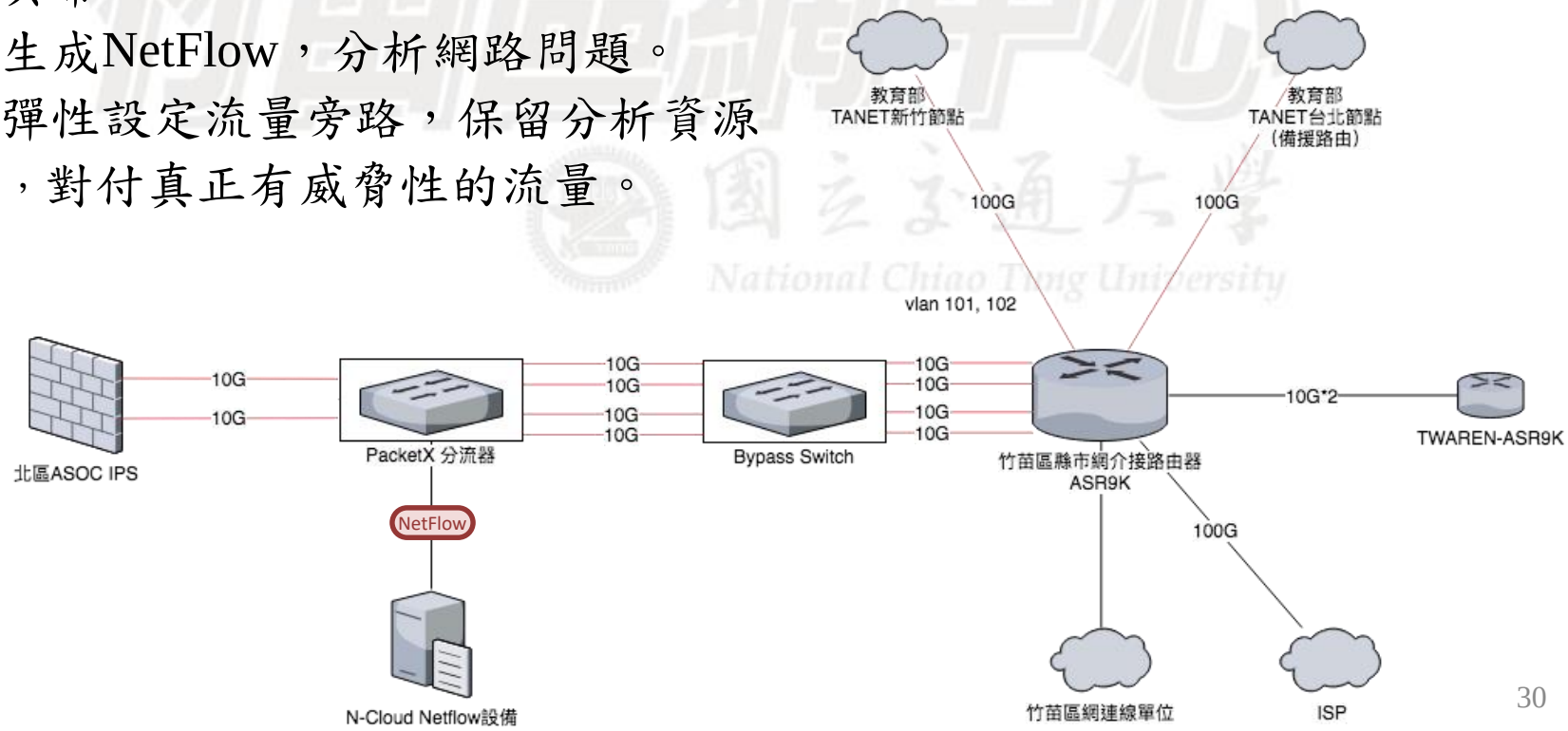


推動網路資訊應用環境之導入情形

–網路資訊安全設備

➢ 北區資訊安全聯防機制

- 透過北區A-SOC計畫建立資訊安全聯防機制。
- 統一監控惡意網路活動，近端阻擋惡意程式，避免造成學術網路流量異常。
- 生成NetFlow，分析網路問題。
- 彈性設定流量旁路，保留分析資源，對付真正有威脅性的流量。

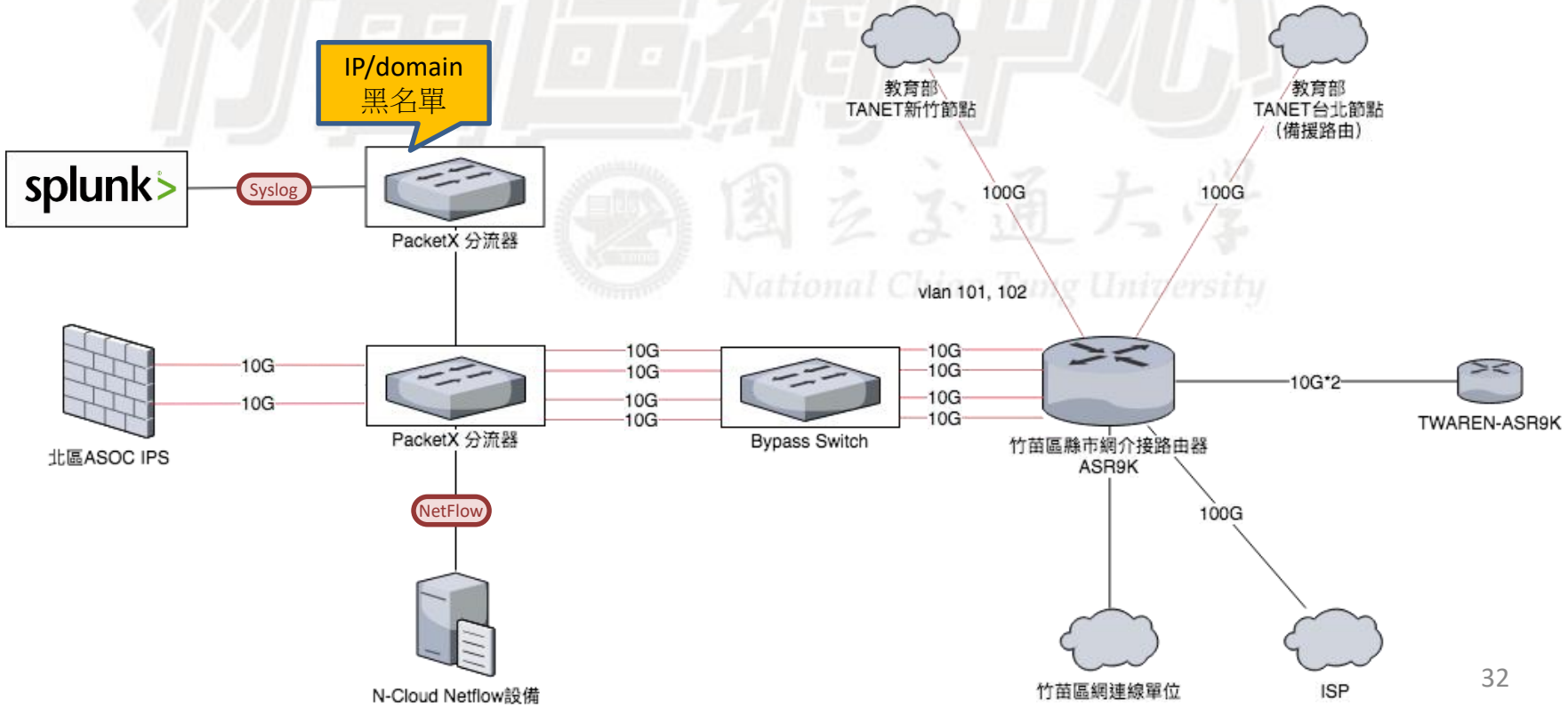


5. 網路應用創新服務情形

- 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
  - 於分流器導入黑名單偵測機制。
  - 提供連線單位1:1流量紀錄分析及查詢
  - 提供CACTI監控系統範本(vsphere 版本)下載。
  - 校園資訊服務節能計畫
  - 建立區網Line群組並提供LineBot通知資安事件
- 到校服務

網路應用與創新服務-導入黑名單偵測機制

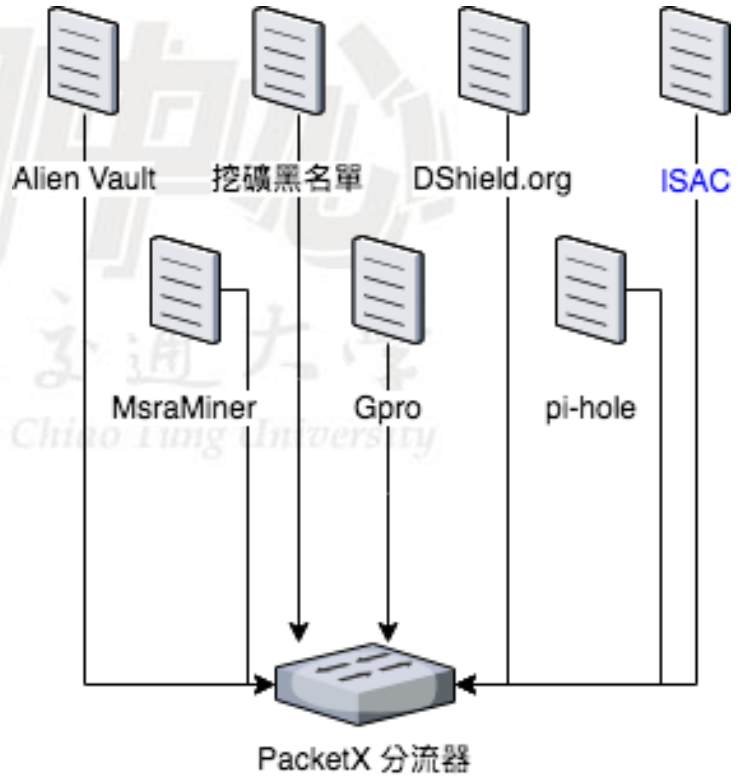
- 北區資訊安全聯防機制再進化
  - 分流器預載黑名單(免費共享情資)，偵測IPS未阻斷的威脅
  - 分流器產生偵測事件Syslog送至Splunk統計分析威脅紀錄



網路應用與創新服務-導入黑名單偵測機制

黑名單來源	IP數量 (63K)	Domain數量 (1.7M)
ALIEN VAULT	63,228	291
挖礦黑名單 (coinhive & 礦池)	-	4652
DShield.org Suspicious Domain List	-	6,000
MsraMiner v2.1	-	4
中華電信資安研究所 domain List(Gpro)	-	472
Porn list from pi-hole	-	1,702,466

黑名單資訊一覽表



網路應用與創新服務-導入黑名單偵測機制

- 資安聯防數據分析

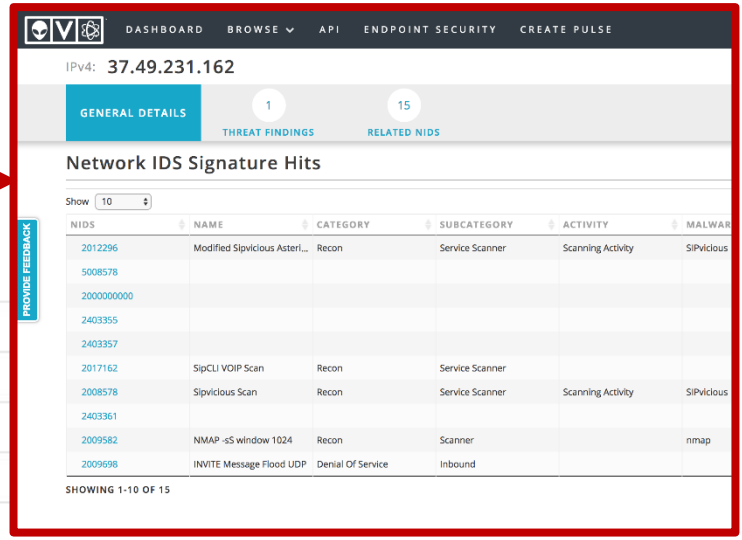
報告

最高值　　依時間的最高值　　罕見值

具有此欄位的事件

最高 10 個值	數量	%
37.49.231.162	[illegible]	18.97%
212.64.111.52	158,196	6.616%
176.119.4.60	78,196	3.27%
118.25.145.88	64,822	2.711%
122.228.19.79	42,007	1.757%
176.119.7.26	37,679	1.576%
176.119.7.30	36,953	1.545%
176.119.4.9	36,919	1.544%
176.119.7.14	35,843	1.499%
176.119.7.34	33,817	1.414%

▲ 資訊安全安全事件紀錄之統計報表



Category:
Recon
Subcategory:
Service Scanner
Malware:
SIPvicious

網路應用與創新服務-導入黑名單偵測機制

- 挖礦數據統計資訊

find_content

61 值, 100% 的事件

報告

最高值　　依時間的最高值

具有此欄位的事件

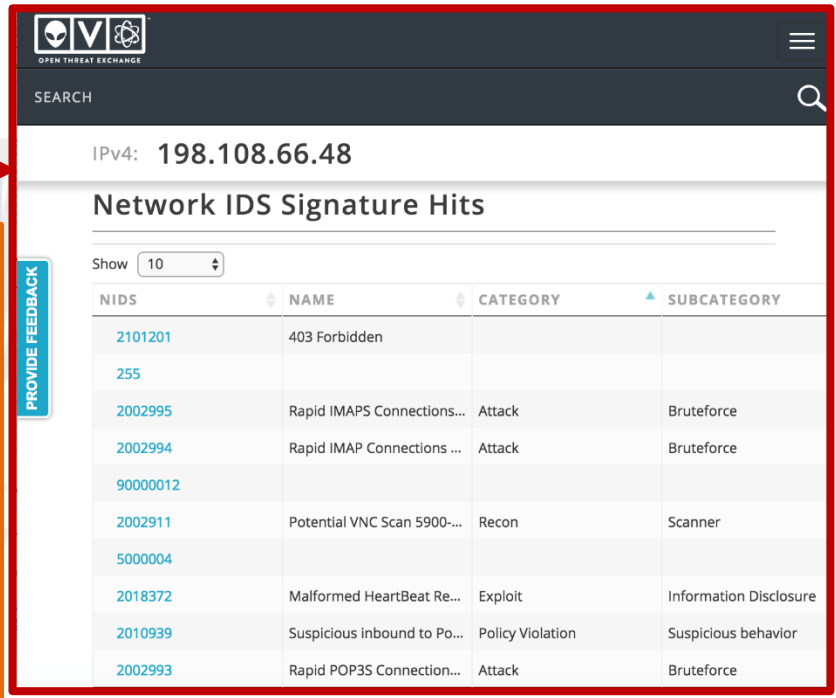
最高 10 個值

gulf.moneroocean.stream		
pool.minexmr.com		
xmr.crypto-pool.fr		
coinhive.com		
player.h-cdn.com	48	0.232%
monero.crypto-pool.fr	30	0.145%
pool.supportxmr.com	30	0.145%
gemius.pl	25	0.121%
freebitco.in	19	0.092%
monerohash.com	18	0.087%

網路應用與創新服務-導入黑名單偵測機制

- 探討Port 443
  - 同為443流量中，發現針對mail server所發動的暴力破密攻擊

i	_time	sip	dip	sport	dport
>	18/11/21 18:10:12.000	108.178.16.154	120.106.207.79	56547	443
>	18/11/21 18:10:12.000	198.108.66.63	120.106.155.162	55697	443
>	18/11/21 18:10:12.000	198.108.66.48	120.106.155.162	33619	443
>	18/11/21 18:10:12.000	5.188.206.249	120.106.17.212	57433	443
>	18/11/21 18:10:12.000	5.188.206.249	120.106.18.17	57433	443
>	18/11/21 18:10:12.000	108.178.16.154	120.104.30.81	58386	443
>	18/11/21 18:10:12.000	108.178.16.154	120.105.102.83	47791	443
>	18/11/21 18:10:12.000	108.178.16.154	163.19.84.183	60495	443
>	18/11/21 18:10:12.000	108.178.16.154	163.19.241.219	46259	443
>	18/11/21 18:10:11.000	108.178.16.154	120.106.86.219	48278	443



Category:
Attack, Exploit
Subcategory:
Bruteforce,
Information Disclosure

網路應用與創新服務-1:1流量紀錄分析及查詢

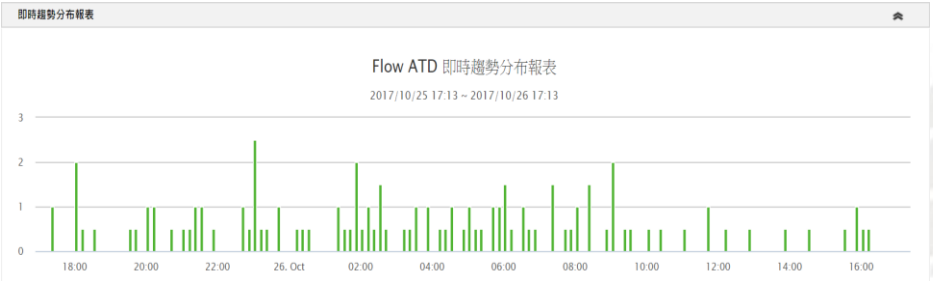
- 除系統內建總管理者領域“Global”領域外，開啟27個領域及所屬帳號，提供連線學校自行查詢分析Netflow。

網路應用與創新服務-1:1流量紀錄分析及查詢

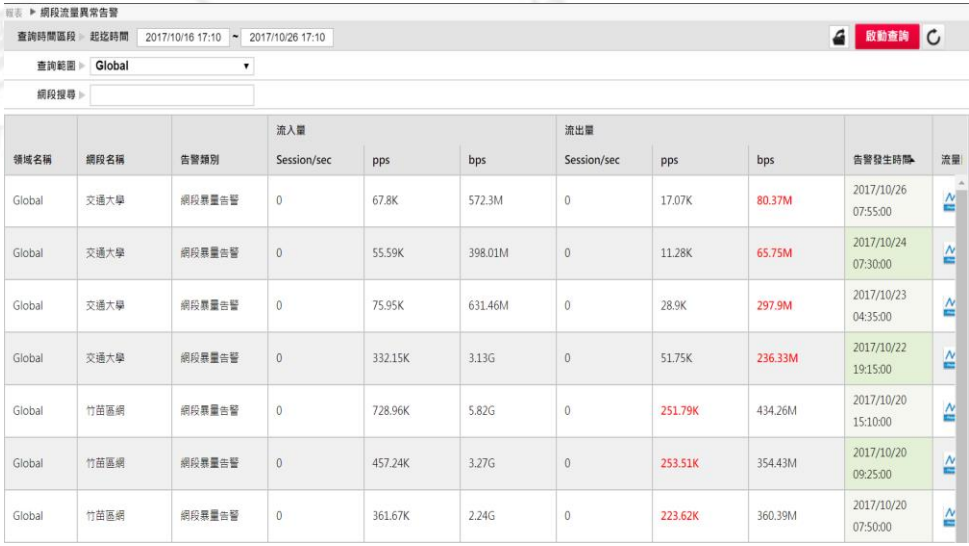
- 已於系統內建立了TopN報表43支、分時監控報表35支。

網路應用與創新服務-1:1流量紀錄分析及查詢

- 系統網段流量異常告警，可以即時掌握DDoS、Host Scan、Port Scan及異常流量等網路行為



所屬領域	異常項目	攻擊者IP	受害者IP	協定	目的P	Session	Packet:	Bytes	開始時間	結束時間	瀏覽
Global	Host Scan	111.75.200.68		TCP	22	21.32K	21.32K	1.37M	2017/10/26 16:18:00	2017/10/26 16:19:00	
Global	Host Scan	210.245.87.33		UDP	5060	33.96K	33.96K	14.85M	2017/10/26 16:11:00	2017/10/26 16:12:00	
Global	Host Scan	183.102.195.234		TCP	1338	26.4K	26.4K	1.55M	2017/10/26 16:01:00	2017/10/26 16:02:00	
Global	TCP SYN Host Scan	183.102.195.234		TCP	1338	10.67K	10.67K	426.91	2017/10/26 15:59:00	2017/10/26 15:59:00	



領域名稱	網段名稱	告警類別	流入量 Session/sec	流入量 pps	流入量 bps	流出量 Session/sec	流出量 pps	流出量 bps	告警發生時間	流量
Global	交通大學	網段暴量告警	0	67.8K	572.3M	0	17.07K	80.37M	2017/10/26 07:55:00	
Global	交通大學	網段暴量告警	0	55.59K	398.01M	0	11.28K	65.75M	2017/10/24 07:30:00	
Global	交通大學	網段暴量告警	0	75.95K	631.46M	0	28.9K	297.9M	2017/10/23 04:35:00	
Global	交通大學	網段暴量告警	0	332.15K	3.13G	0	51.75K	236.33M	2017/10/22 19:15:00	
Global	竹苗區網	網段暴量告警	0	728.96K	5.82G	0	251.79K	434.26M	2017/10/20 15:10:00	
Global	竹苗區網	網段暴量告警	0	457.24K	3.27G	0	253.51K	354.43M	2017/10/20 09:25:00	
Global	竹苗區網	網段暴量告警	0	361.67K	2.24G	0	223.62K	360.39M	2017/10/20 07:50:00	

網路應用與創新服務-1:1流量紀錄分析及查詢

- 竹苗區網總管理者可以即時透過Global查詢區網所有流量資訊，各領域管理者也能透過領域權限查詢到所屬領域相關流經區網中心的流量紀錄，中心管理者透過模擬領域功能即時協助各領域檢視相關資訊

來源IP	來源區域	來源Port	來源Port解析	Protocol	目的IP	目的IP名稱解析	目的區域	目的Port	Session	Packets	Bytes	TCP Flag	目的AS
148.251.152.24	DE	21	ftp	TCP			TW	53680	1	1	40	-A---F	18420 (National Cent
121.129.43.29	KR	4311		TCP			TW	8775	1	2	80	-A---F	18420 (National Cent
75.126.182.37	US	80	http	TCP			TW	60497	1	16	19.56K	-AP--F	18420 (National Cent
107.191.45.89	US	22	ssh	TCP			TW	42847	1	15	3.23K	-AP-SF	18420 (National Cent
34.236.88.28	US	80	http	TCP			TW	50868	1	3	132	-A---F	9916 (National Chiao
77.72.83.235	GB	59532		TCP			TW	40002	1	2	80	---RS-	9916 (National Chiao
183.136.202.244	CN	18558		TCP			TW	1433	1	5	394	-AP-SF	18420 (National Cent
120.117.3.61	TW	80	http	TCP			TW	8971	1	66	86.5K	-AP-SF	131591 (Ambit Micro Corporation,TW)

台聯大	ustedu
交通大學	nctu
HCRC-明新科大	must
HCRC-玄奘大學	hcu
HCRC-元培科大	ypu
HCRC-大華科大	tust

網路應用與創新服務-1:1流量紀錄分析及查詢

- 除了收集區網中心NetFlow外，也可以透過Syslog及SNMP協定將中心端重要主機設備的Syslog、SNMP一併收攏，一套系統即可達到Flow、Syslog、SNMP的資料收集及保存，省去額外建置Log Server、網管軟體的高額建置費用

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

CACTI VM下載連結網址：

https://www.hcrc.edu.tw/other/download/system_download/

本年度已協助建置完成單位
新竹高中
世界高中

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 11 of 11 [1] | Next >>

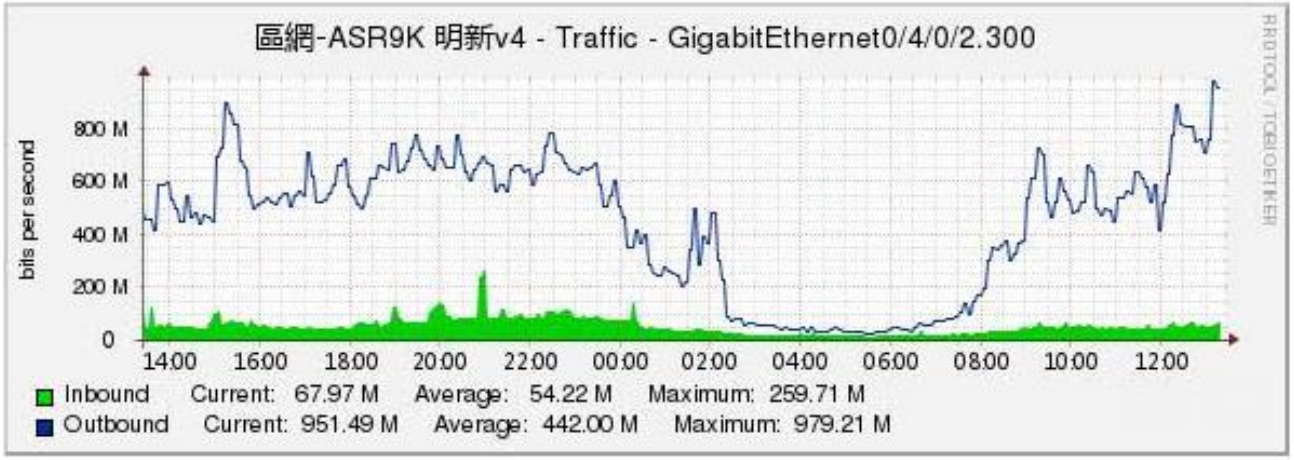
Actions	Name	ID	Type	Trigger	Duration	Repeat	Warn Hi/Lo	Alert Hi/Lo	BL Hi/Lo	Current	Triggered**	Enabled
	區網-ASR9K - 新竹高中 - GigabitEthernet0/4/0/15 [traffic_in]	84	High/Low	1 Minute	N/A	Never	900/-	-/0.001	N/A	241,212.4333	yes	Enabled
	區網防火牆-PA5060 - Total Active Sessions [pan_ses_activ]	13	High/Low	1 Minute	N/A	Every 10 Minutes	1000000/-	800000/-	N/A	21606	no	Enabled
	區網-ASR9K - 明新v4 - GigabitEthernet0/4/0/2.300 [traffic_out]	77	High/Low	1 Minute	N/A	Never	900/-	-/0.001	N/A	308.1532	no	Enabled
	區網-ASR9K - 明新v4 - GigabitEthernet0/4/0/2.300 [traffic_in]	78	High/Low	1 Minute	N/A	Never	900/-	-/0.001	N/A	49.7611	no	Enabled
	區網-ASR9K - 聯合 - GigabitEthernet0/4/0/3 [traffic_out]	79	High/Low	1 Minute	N/A	Never	900/-	-/0.001	N/A	389.4771	no	Enabled
	區網-ASR9K - 聯合 - GigabitEthernet0/4/0/3 [traffic_in]	80	High/Low	1 Minute	N/A	Never	900/-	-/0.001	N/A	37.684	no	Enabled
	區網-ASR9K - 新竹高商 - GigabitEthernet0/4/0/13 [traffic_out]	81	High/Low	1 Minute	N/A	Never	900/-	-/0.001	N/A	84.3296	no	Enabled
	區網-ASR9K - 新竹高商 - GigabitEthernet0/4/0/13 [traffic_in]	82	High/Low	1 Minute	N/A	Never	900/-	-/0.001	N/A	14.0443	no	Enabled
	區網-ASR9K - 新竹高中 - GigabitEthernet0/4/0/15 [traffic_out]	83	High/Low	1 Minute	N/A	Never	900/-	-/0.001	N/A	21.6131	no	Enabled
	區網-ASR9K - 光復中學 - GigabitEthernet0/4/0/14 [traffic_out]	85	High/Low	1 Minute	N/A	Never	900/-	-/0.001	N/A	37.4179	no	Enabled
	區網-ASR9K - 光復中學 - GigabitEthernet0/4/0/14 [traffic_in]	86	High/Low	1 Minute	N/A	Never	900/-	-/0.001	N/A	6.3426	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：本個案預設頻寬警戒值設定為900Mbits，目前流量為914.0121Mbits，系通將會自動發送下列訊息至單位網管人員。

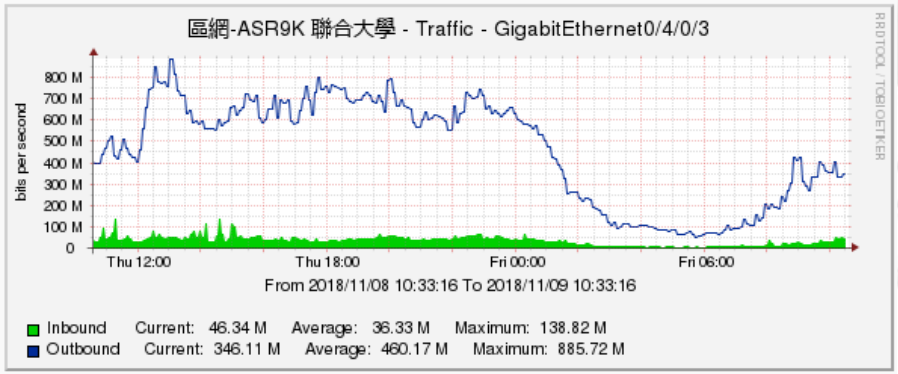
Host: 區網-ASR9K (192.192.60.113)
URL: http://163.28.64.84/cacti//graph.php?local_graph_id=214&rra_id=1
Message: WARNING: 區網-ASR9K - 明新v4 - GigabitEthernet0/4/0/2.300 [traffic_out] [traffic_out] went above threshold of 900 with 914.0121

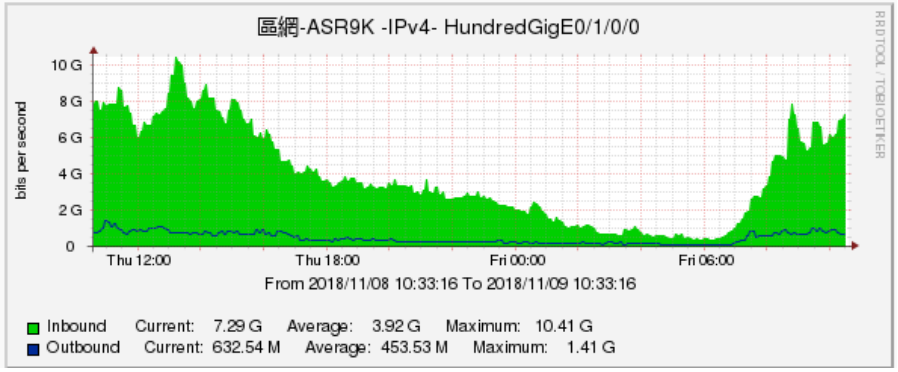


網路應用與創新服務-監控系統

CACTI監控系統—每日流量使用提醒

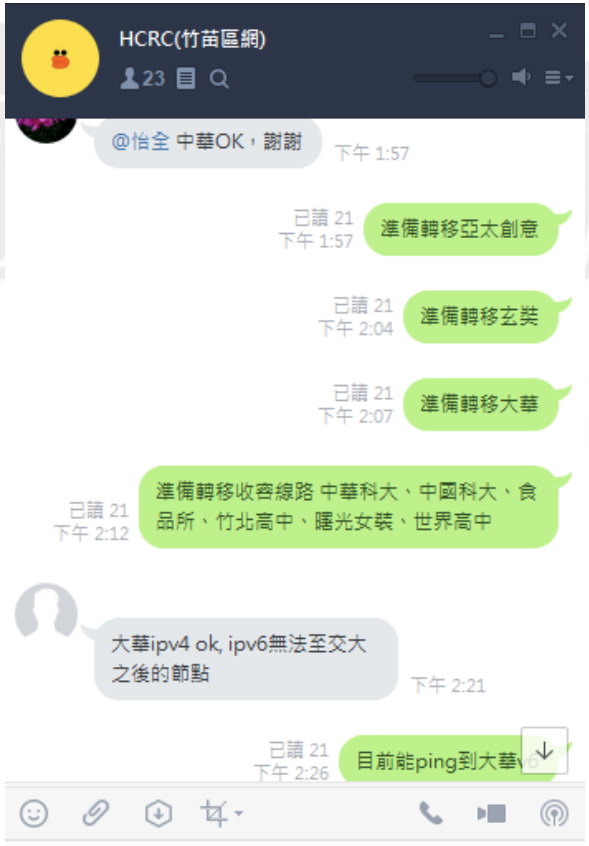
範例：各單位獨立設定網路流量圖，於每日上午08:30自動寄信通知單位網管老師前一日網路使用情形。

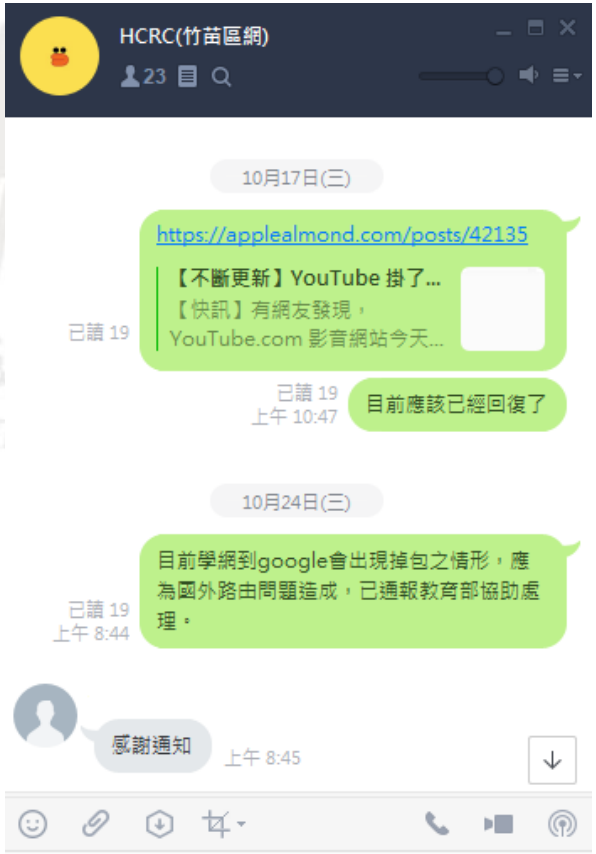




網路應用與創新服務-建立區網Line群組

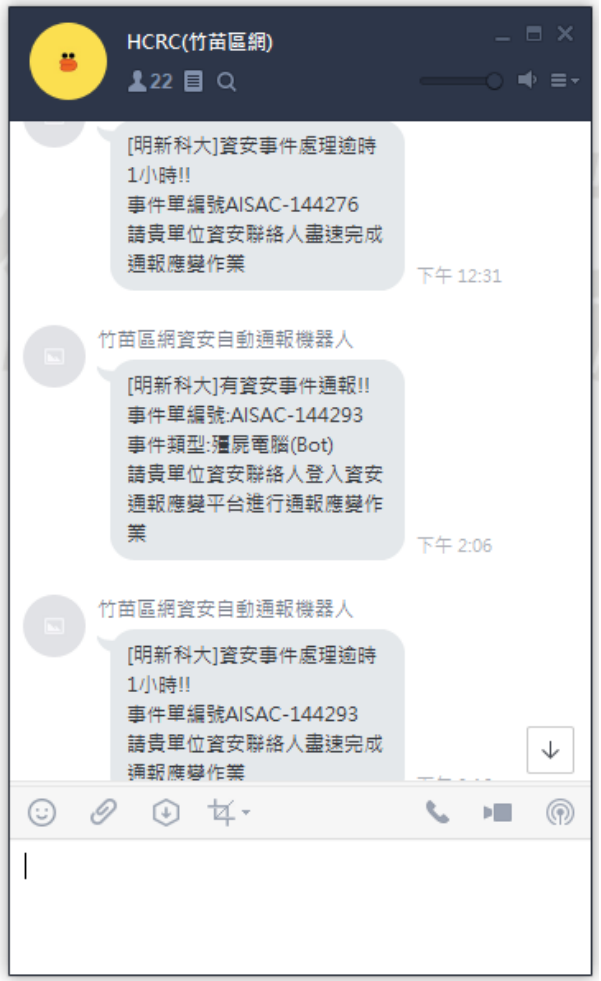
- 建立區網Line群組，能透過群組向連線單位即時提供資訊，並能讓區網夥伴快速反應問題。





網路應用與創新服務-建立區網Line群組

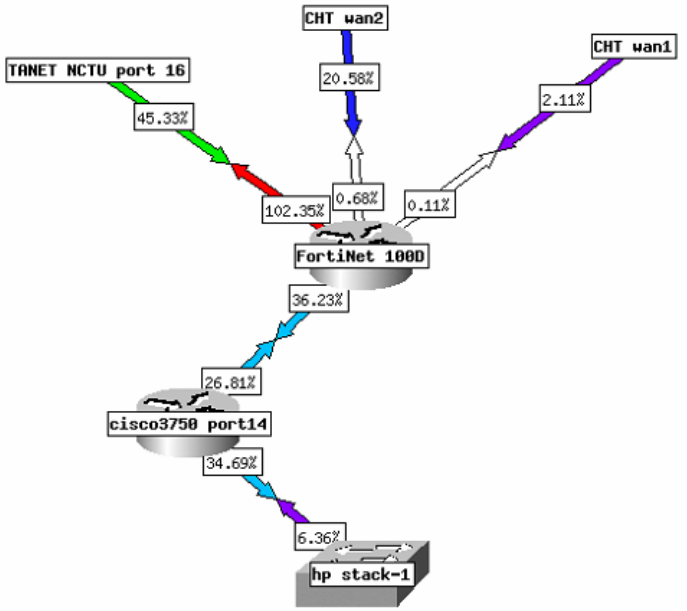
- 建立LineBot資安通報機器人，能在連線單位有資安通報時於Line群組即時通知該單位儘快處理。



竹苗區網到校服務

本年度協助單位:

1. 協助導入IPv6網路環境：
   校網頁及DNS支援IPv6：
   世界高中
2. 協助建置Cacti監控系統：
   世界高中、新竹高中



6. 辦理教育訓練及推廣活動情形

本年度針對區網連線單位網管人員已舉辦13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300位網管人員，本年度邀請南投區網及高雄市教網的老師前來做跨區網技術分享。

日期	活動名稱
107年03月06日	資訊安全實務
107年06月26日	全方位資訊安全防護-理論與實務
107年09月17日	Syslog-Netflow 分析管理平台
107年09月21日	Syslog-ng系統事件收集系統
107年10月01日(上)	DNS概念與DNS服務主機實作(上)
107年10月01日(下)	DNS概念與DNS服務主機實作(下)
107年10月11日	手機網路安全防護
107年10月12日	雲端安全管理

辦理教育訓練及推廣活動情形

日期	會議	議題
107年03月06日	竹苗區網第一次管委會	1. 竹苗區網架構變更說明 2. Line及資安通報機器人建立說明
107年10月11日	竹苗區網第二次管委會	1. 竹苗區網架構變更成果說明 2. 區網提供Syslog-Netflow分析平台 3. 推動EVS網頁弱點掃描平台

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2017年7月前重新驗證ISMS	本年度4月26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	新竹高中 世界高中
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3所連線學校進行網站弱點掃描
協助至少一所連線單位導入IPv6功能。	世界高中

8. 經費運用情形

教育部補助經費： 1,360,000 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%

自籌經費：0元

9. 結語與綜合建議

1. 已於本年度完成骨幹設備連線模組升級，並完成架構的簡化調整，將持續提供優質網路服務。
2. 完成汰換資訊機房B迴路之老舊UPS，減少電力耗損,，增進節能效益。
3. 已建立區網Line群組及Line資安通報機器人，持續提升區網資安事件處理效率及服務品質。
4. 本年度針對區網連線單位網管人員已舉辦13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300位網管人員，109年度將持續舉辦以提升各單位網管人員相關資訊能力。

9. 結語與綜合建議

5. 目前因分流器處理流量上限為10G，形成網路瓶頸點，若流量持續成長，則須提升分流器處理上限至20G。
6. 建議協助區網中心建置DDoS偵測及清洗設備，以提供連線單位更即時的DDoS防護。
7. 部分連線單位反應連接至區網中心之線路租金過於高昂且網路速度也不盡理想，相較於與縣市網連接之性價比較差。

10.108年度預計推動之重點工作

- 提供流量分析系統，幫助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，並提供DNS備援供各連線單位使用。
- 持續推動各單位於DNS及網頁服務導入IPv6。
- 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。
- 持續精進技術能量並於區網做技術分享。
- 視需求將安排資安、網路相關課程。
- 推動資安認證，提升資安認證數。

報告完畢
敬請指教

Thanks!