

北區 A-SOC 進度及問題

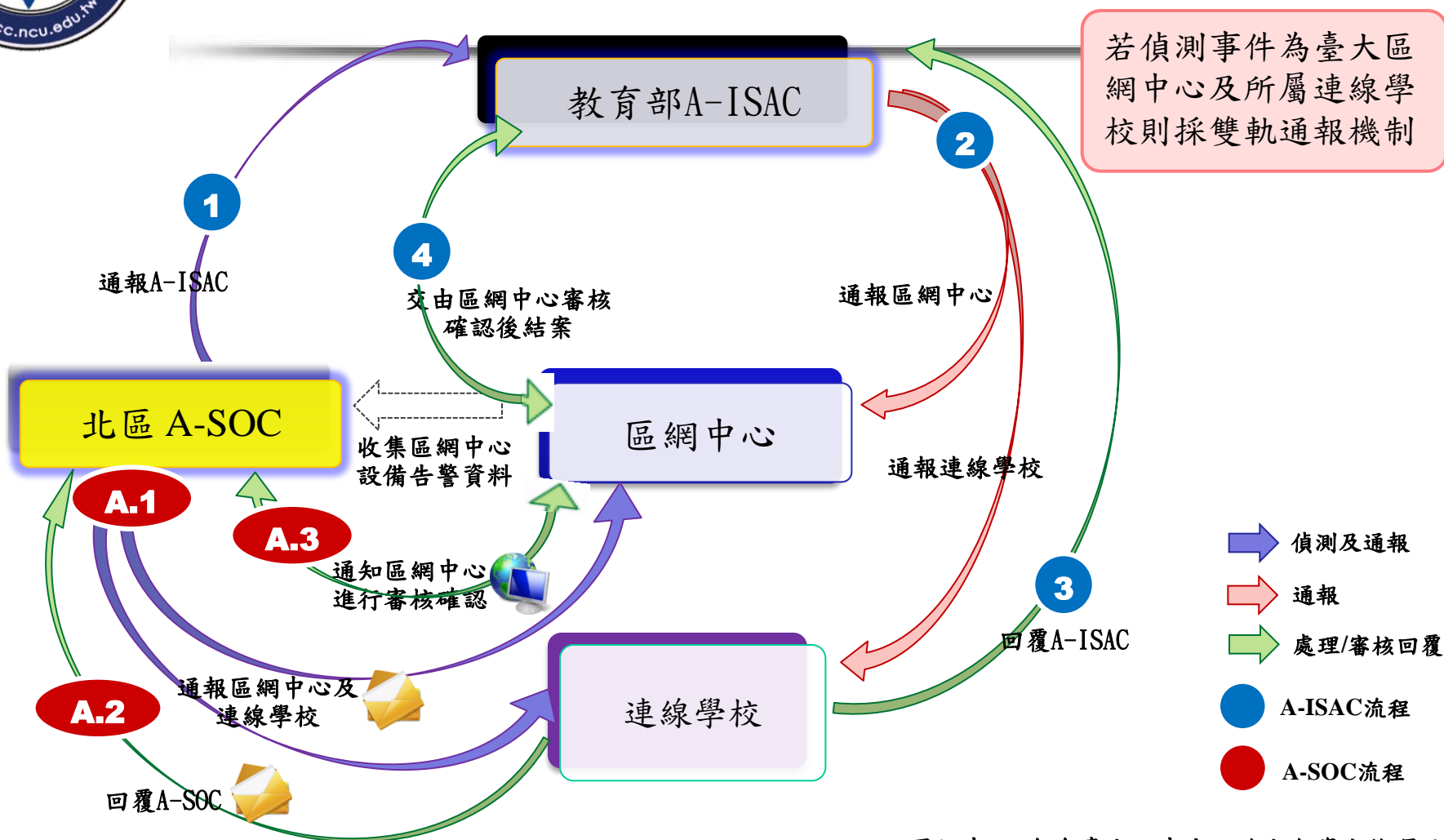
國立中央大學電算中心
100年8月17日



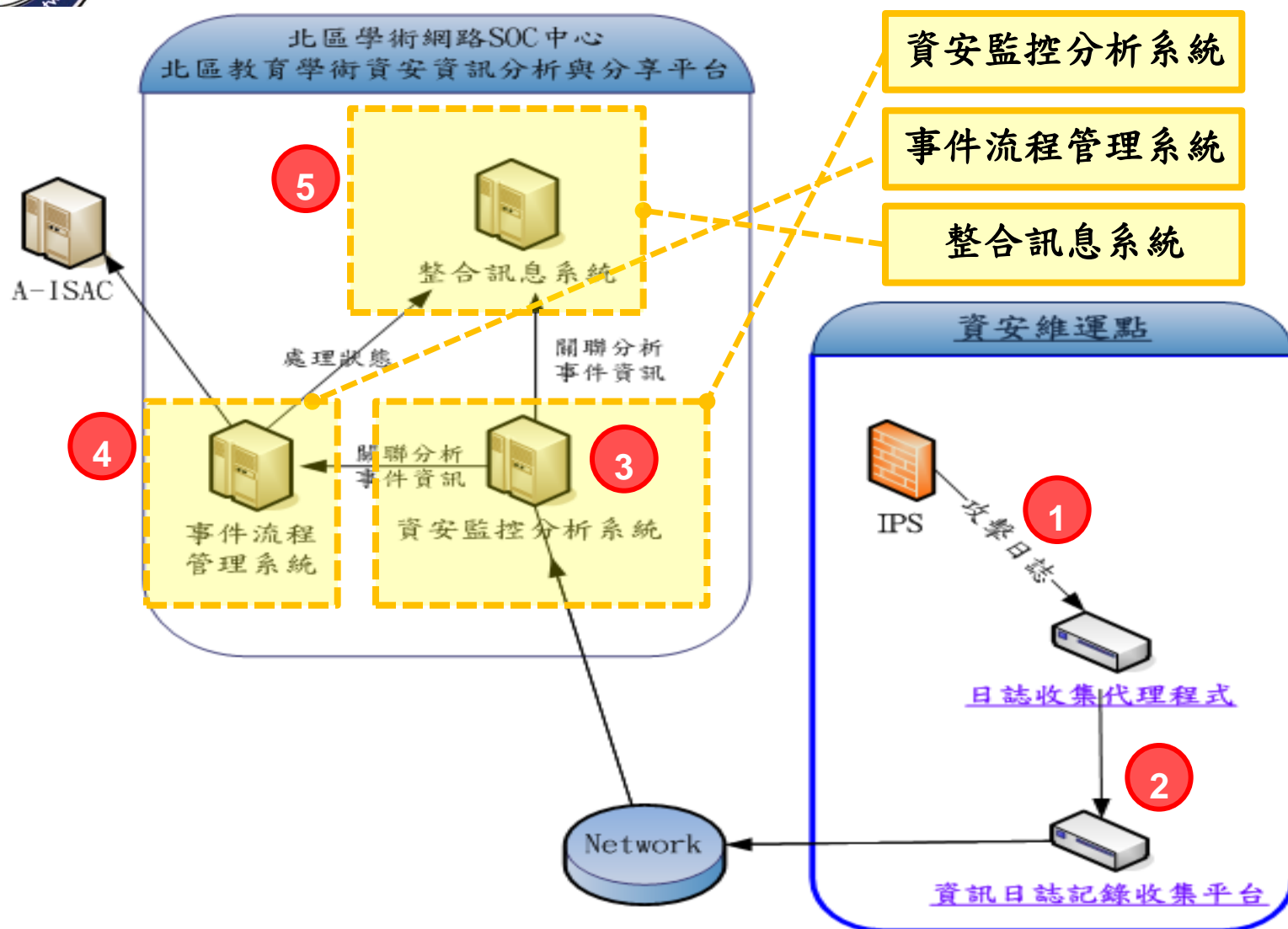
報告大綱

- ☐ 北區A-SOC系統運作
- ☐ 建置IPS後之問題

北區A-SOC事件通報處理流程-7/1啟動



資安事件觸發系統監控情境示意圖





資安事件關聯分析類別

- ❑ 客製監控資安事件
 - 技服中心惡意網域/IP 事件
 - 網頁掛馬/竄改
 - ...
- ❑ 達門檻值事件(統計)
 - 內部主機進行Bot連線 (5分鐘5次)
 - 網頁伺服器遭阻斷服務攻擊 (1分鐘100次)
 - ...
- ❑ 異質設備關聯事件
 - PortScan大量掃描(防火牆有大量連線且IPS有Scan資安事件)
 - ...



整合訊息系統入口網站

SOC 北區學術資訊安全維護中心

163.28.16.25/portal.php

北區學術資訊安全維護中心

Academic Security Operation Center

首頁 | 關於 A-SOC | 訊息公告 | 資安預警情報 | 整合訊息系統

事件來源地理分析

Google 使用條款

事件來源國家排名

排名	國家	城市	事件數
1	Taiwan	Taipei	312
2	China	Beijing	85
3	Taiwan	Taoyuan	81
4	China		27
5	China	Shenzhen	24
6	Taiwan		24
7	Korea, Republic of	Seoul	22
8	United States	Absecon	16
9	Russian Federation		13
10	China	Shanghai	12

※資料來源: 2011年07月北區ASOC事件來源IP

資安預警情報

網路安全事件簿

- 2011-08-09 資安訊息: 七月份網路安全威脅報告
- 2011-07-06 資安訊息: 六月份網路安全威脅報告

網路安全新聞

- 2011-08-15 手機app有漏洞 谷歌否認
- 2011-08-15 駭客德國大會師 挑戰維解

更多...

相關連結

- A-ISAC
- 台北區網中心
- 台北區網中心

顯示所有下載...



整合訊息系統登入

整合訊息系統

帳號 Account

密碼 Password

登入 重設

Copyright © 2011 北區學術資訊安全維運中心
Academic Security Operation Center - All Rights Reserved
TEL: (02) 3366-5009 | email: ntuasoc@ntu.edu.tw



整合訊息系統首頁

可看到今日監控範圍發生哪些資安事件(中風險事件9個、低風險事件13個)、過去一週日事件量約50~75左右

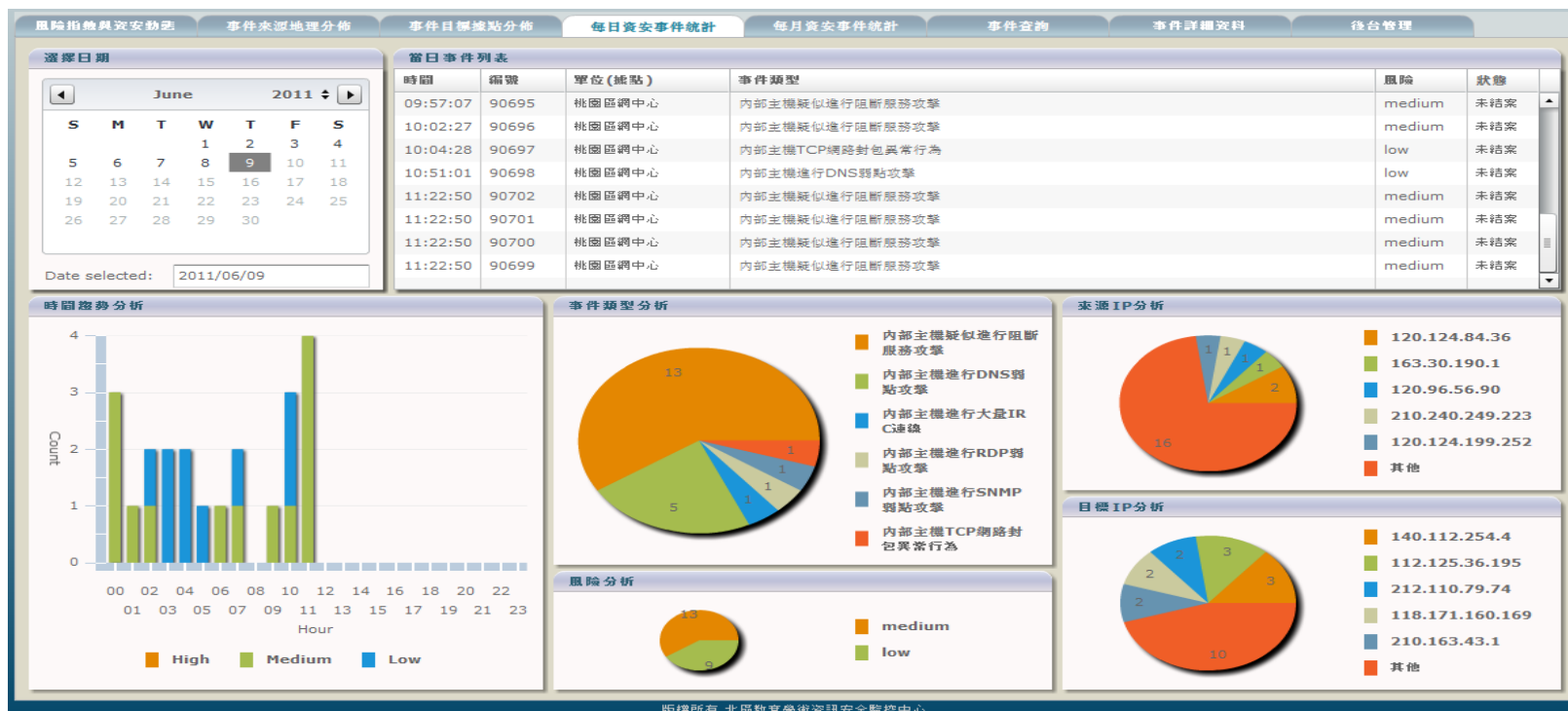


版權所有 北區教育學術資訊安全監控中心



整合訊息系統日報表

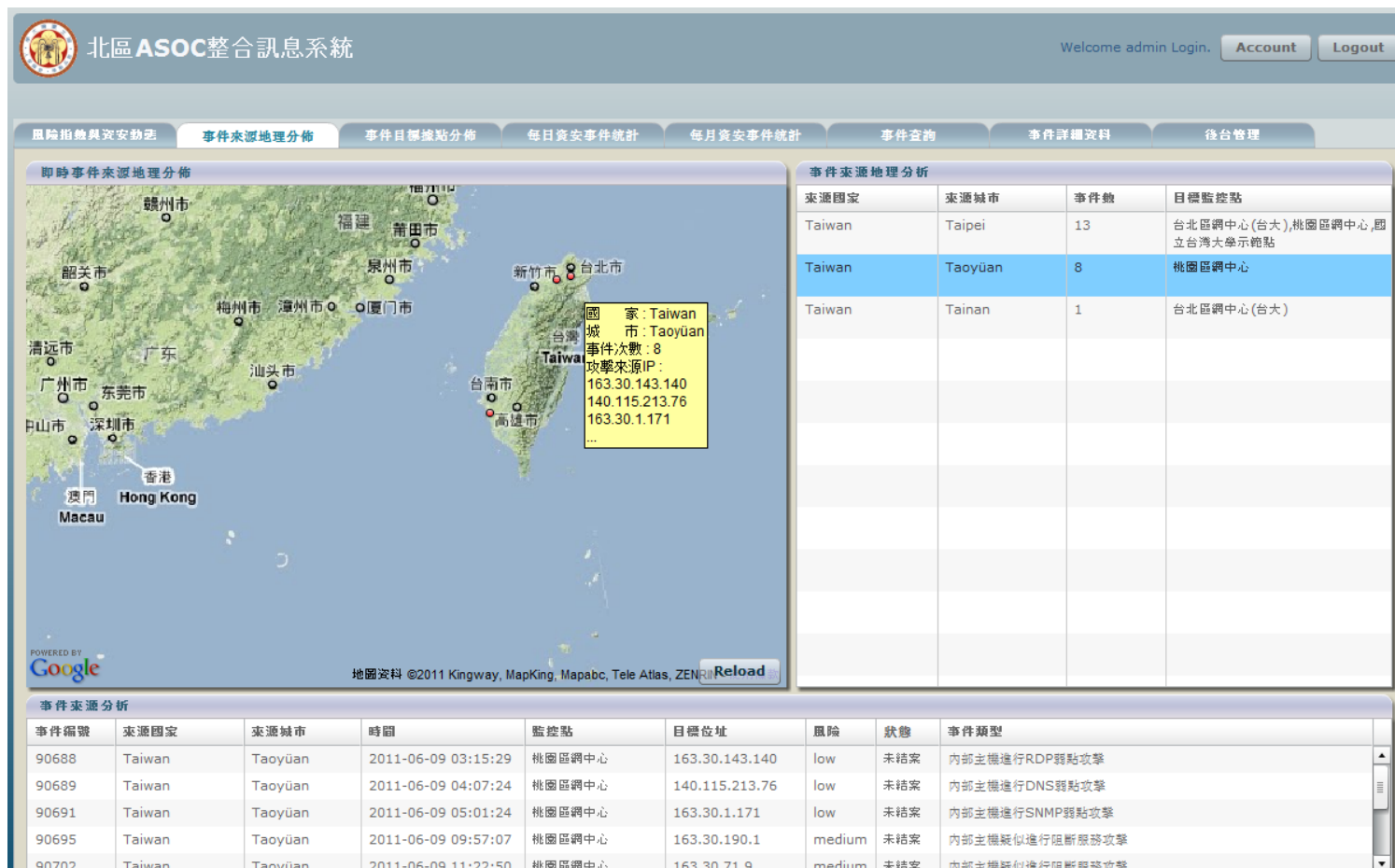
查看日報表可發現當日事件於每小時的走勢、事件多為內部主機疑似進行阻斷服務攻擊及DNS弱點攻擊





整合訊息系統事件來源地理資訊

□ 今日事件來自台北、桃園、台南

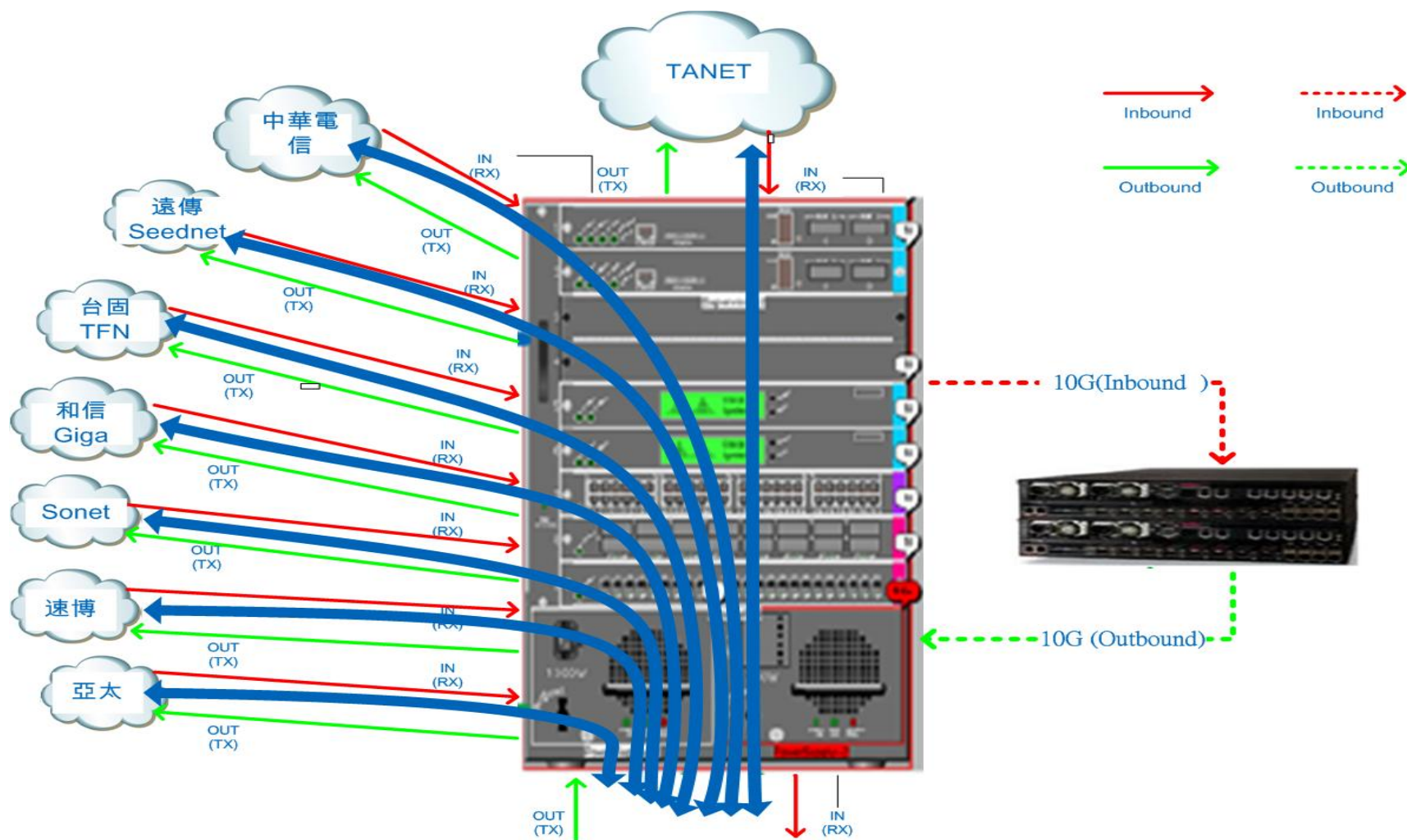




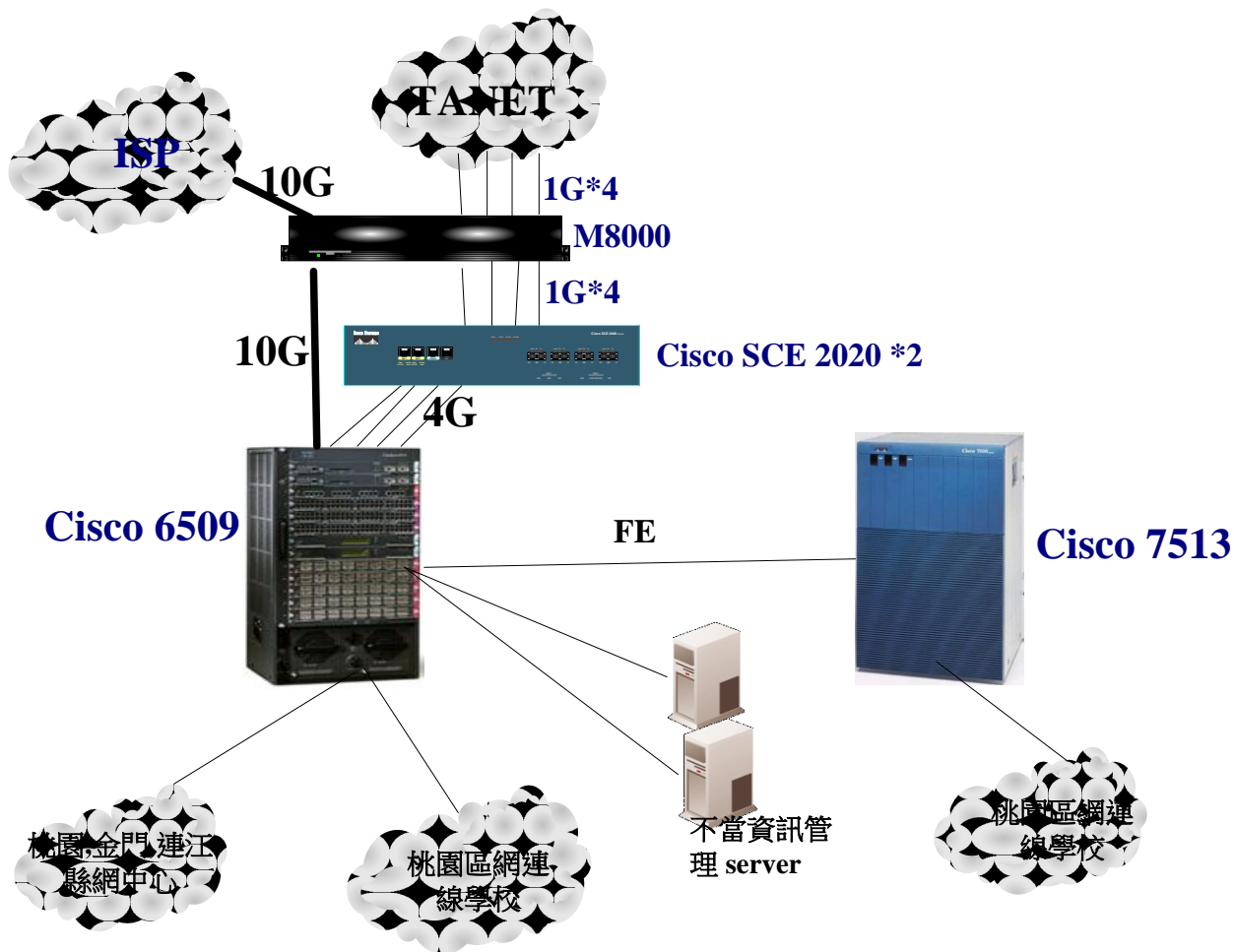
問題

- ☐ 在5/7 23:40 到5/8 00:40 桃園區網到tanet 骨幹斷線
- ☐ 6/30 09:40 ~10:00 骨幹斷線
- ☐ 7/20 15:10 ~15:50 區網對外網路連線緩慢
- ☐ 解決:bypass IPS及clear arp

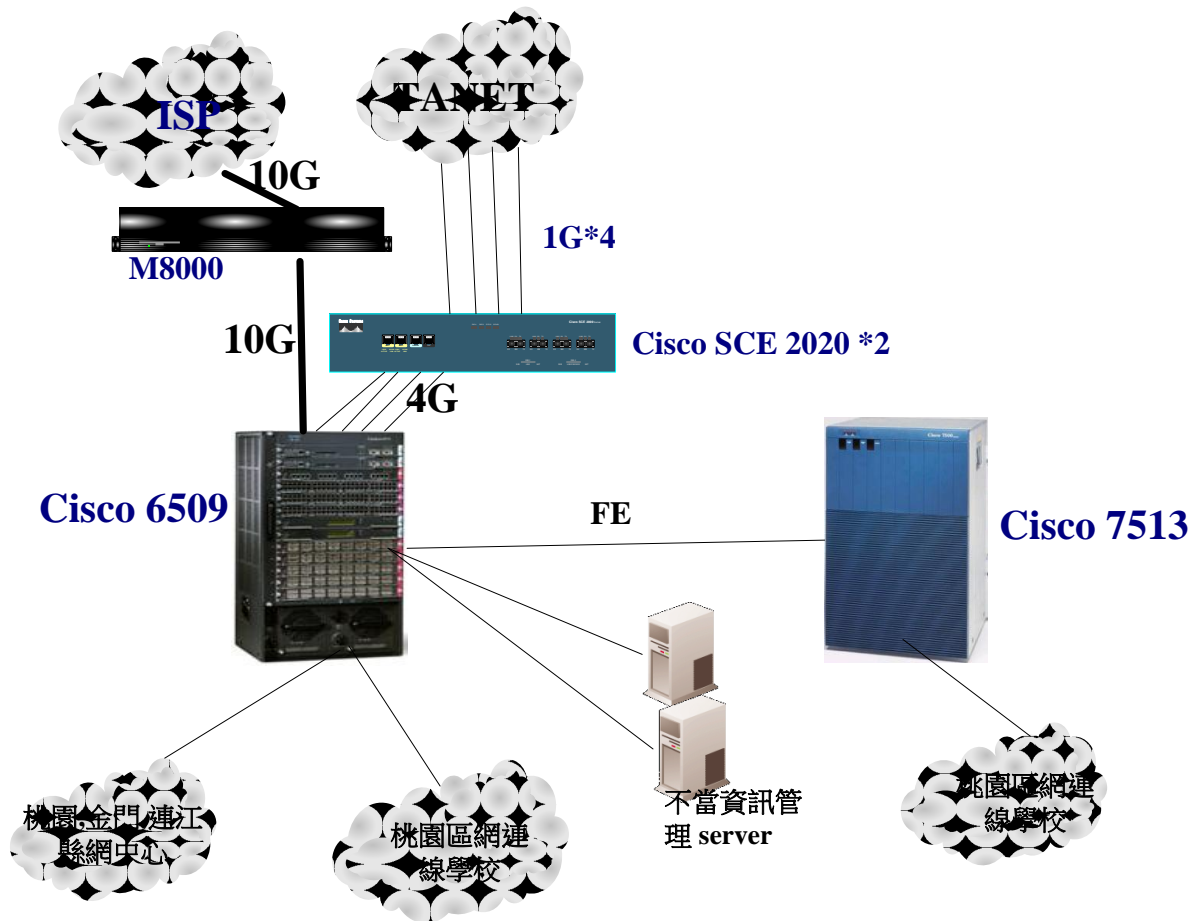
桃園區網IPS規劃架構



IPS 架構調整-Tanet骨幹



IPS 架構調整-目前





Computer Center, National Central University.



Thank You!