

雲嘉區域網路中心營運持續計畫 演練成果報告

情境一

日期：99.10.22



情境內容

- 區網中心負責網路維運人員，因感染流行性疾病，導致無法到校上班。
- 區網中心骨幹路由器發生異常，導致雲嘉區域網路電路異常斷訊。
- 依現況啟動備援機制由職務代理人執行復原工作。



演練前會議

- 演練前演練小組召集人邀集區網維護TANet網路骨幹維運相關人員召開演練前說明會議。
- 區網維運業務負責人員說明此次營運持續計畫演練內容及目的。



會議進行狀況

- 參與演練人員熱烈討論演練內容及細節。
- 備援人力說明其角色扮演及執行程序。



宣佈演練開始

- 會議中維運人員核對演練開始時間。
- 會議討論完畢後，主席正式宣佈演練開始，並請參與演練之人員就定位。



維運人員接獲網路異常狀況通知

- 維運人員接獲使用者通知網路異常狀況報告。
- 維運人員進行網路狀況了解，發現TANet骨幹網路異常，立即透過電話通知職務代理人進行網路異常處理。

```
140.123.8-PC1V
> netstat
----- 電腦中心主機系統 -----
www.ccu.edu.tw
PING herci.ccu.edu.tw (140.123.8.8): 56 data bytes
64 bytes from 140.123.8.8: icmp_seq=0 ttl=63 time=0.374 ms

--- herci.ccu.edu.tw ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.374/0.374/0.374/0.000 ms

wstgoang.ccu.edu.tw
PING 140.123.8.118 (140.123.8.118): 56 data bytes
64 bytes from 140.123.8.118: icmp_seq=0 ttl=63 time=0.383 ms

--- 140.123.8.118 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.383/0.383/0.383/0.000 ms

lanming.ccu.edu.tw
PING 140.123.2.86 (140.123.2.86): 56 data bytes
64 bytes from 140.123.2.86: icmp_seq=0 ttl=64 time=0.249 ms

--- 140.123.2.86 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.249/0.249/0.249/0.000 ms

140.123.8.109
PING 140.123.8.109 (140.123.8.109): 56 data bytes
64 bytes from 140.123.8.109: icmp_seq=0 ttl=63 time=0.241 ms

--- 140.123.8.109 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.241/0.241/0.241/0.000 ms
```



職務代理人接獲通報

- 區網職務代理人接獲維運人員電話通知TANet骨幹網路異常狀況報告，請求協助處理。
- 代理人登入主機執行netmon指令(內含tracert、ping之sh script)，並登入6509路由器檢查網路狀況。



網路通訊設備檢查

- 職務代理人及區網維運人員進入機房檢查路由器等實體設備。
- 詳細檢查面版電源指示燈、運作燈號、風扇、網路模組狀況及光纖線路等是否正常運作或脫落？



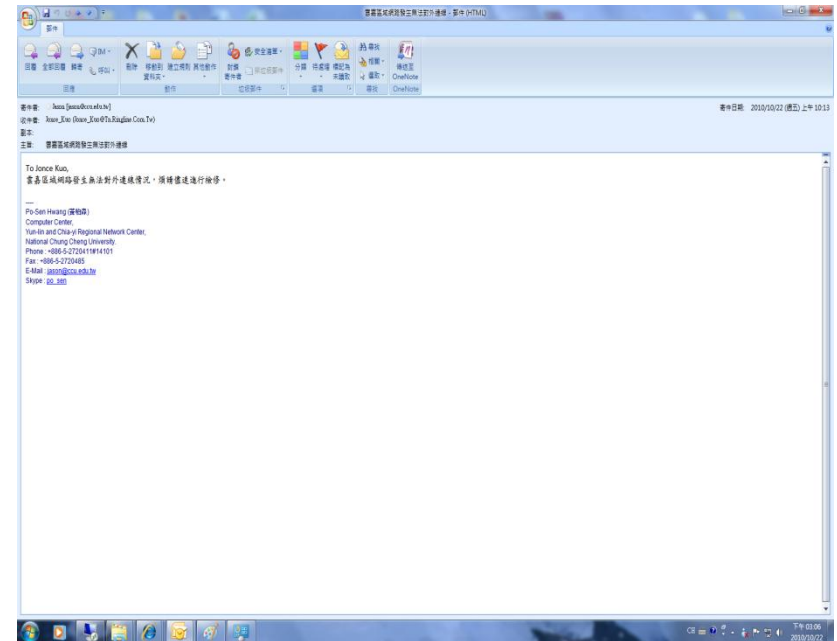
路由器網路狀況檢查

- 代理人員透過筆記型電腦連接6509路由器，以指令檢測路由相關設定，發現Routing Table異常。



通報TANet設備維護廠商

- 以E-mail及電話同時通知TANet維護廠商（麟瑞公司），儘速進行修復。



進行資安通報

- 代理人員判定為資訊安全事件，並以電話通知資訊安全官及單位主管。



資訊安全事件報告單

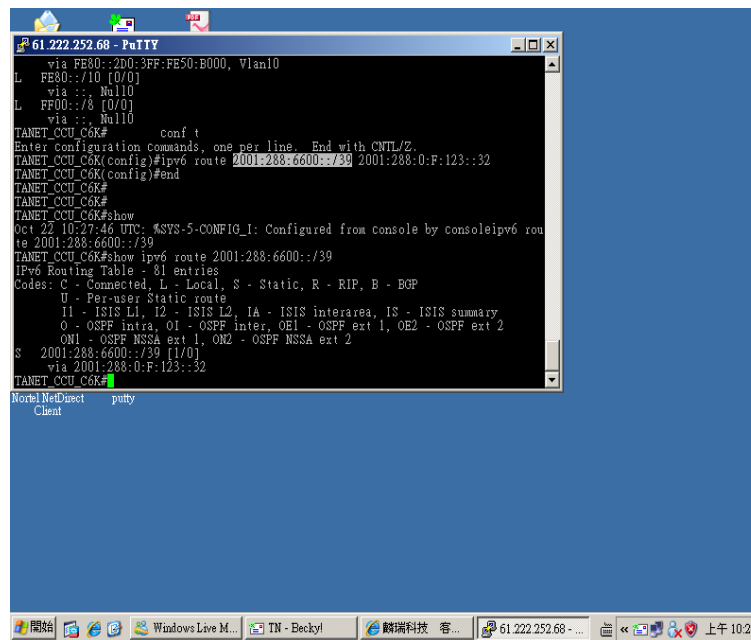
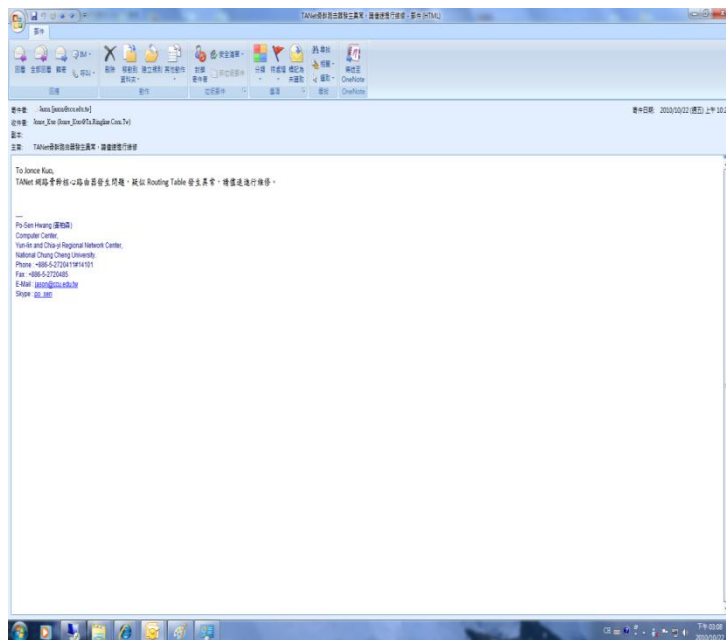
- 由區網網路維運人員依現況填報資安訊安全事件報告單並由資訊安全官簽核確認。

資訊安全事件報告單					
文件編號	RNC-CCU-D-035	機密等級	限閱	版次	1.1
紀錄編號：099-001		填表日期：99年10月20日			
一、發生資訊安全事件之單位聯絡資料：					
單位名稱：國立中正大學電算中心 通報人：黃柏森					
電話：05-2720480 傳真：05-2720485 E-mail：jason@ccu.edu.tw					
二、資訊安全事件通報事項：					
1. 事件發生時間：99年10月22日10時00分					
2. 設備資料：					
◎IP位址 (IP Address)：140.123.12.251 (無；可免填)					
◎網際網路位址 (Web-URL)： (無；可免填)					
◎設備廠牌、機型：Cisco 6509					
◎作業系統名稱、版本：Cisco IOS 12.2(18)SXF4R					
◎已裝置之安全機制：SCE2020					
3. 資訊安全事件資料：					
◎系統安全等級： <input type="checkbox"/> 4級； <input checked="" type="checkbox"/> 3級； <input type="checkbox"/> 2級； <input type="checkbox"/> 1級					
◎影響等級：4級：影響公共安全、社會秩序、人民生命財產。					
3級：系統停頓、業務無法運作。					
2級：業務中斷，影響系統效率。					
1級：業務短暫停頓，可立即修復。					
◎事件分類： <input type="checkbox"/> 非法入侵； <input type="checkbox"/> 感染病毒； <input type="checkbox"/> 阻斷服務； <input checked="" type="checkbox"/> 其他：網路無法連線					
◎破壞程度： <input type="checkbox"/> 系統當機； <input type="checkbox"/> 資料庫毀損； <input type="checkbox"/> 網頁遭篡改； <input checked="" type="checkbox"/> 其他：網路服務中斷					
◎事件說明：(文字勿超過100中文字，標點符號請用大寫) 區網中心 TANet 網路骨幹核心路由器發生故障，導致雲嘉區域網路不通，且負責網路骨幹維護之同仁，因感染流行性感冒而無法到校上班，此時啟動人力備援機進進行緊急處理，並立即進行通報作業，維護廠商進行搶修並回報處理狀況，代理人員確認網路回復正常，最後進行資訊安全事件之檢討。					
◎可能影響範圍及損失評估：(文字勿超過100中文字，標點符號請用大寫) 影響範圍為雲嘉區網連線學校及本校，損失為區域內各單位無法對外傳遞訊息及作業。					
◎應變措施：(文字勿超過100中文字，標點符號請用大寫) 啟動本中心備援人力機置，維護廠商進行路由備份恢復作業並進行資料及網路測試。					
三、期望支援項目：(文字勿超過100中文字，標點符號請用大寫) 希望維護廠商隨時建立路由設備應有備品，確保網路暢通及使用者權益。					
四、解決辦法：(文字勿超過100中文字，標點符號請用大寫) 回復原備份之路由表設定檔後運作正常。					
五、已解決時間：99年10月22日10時41分					
權責單位	單位	會辦	單位	資訊安全官	
黃柏森				李新法	
組長 王鐵雄					



TANet維護廠商接獲通知

- 麟瑞公司接獲電話及E-mail通知路由異常狀況。
- 廠商透過ADSL遠端進入系統，進行系統整體檢查，發現的確是routing table出現錯誤，並進行修復工作。

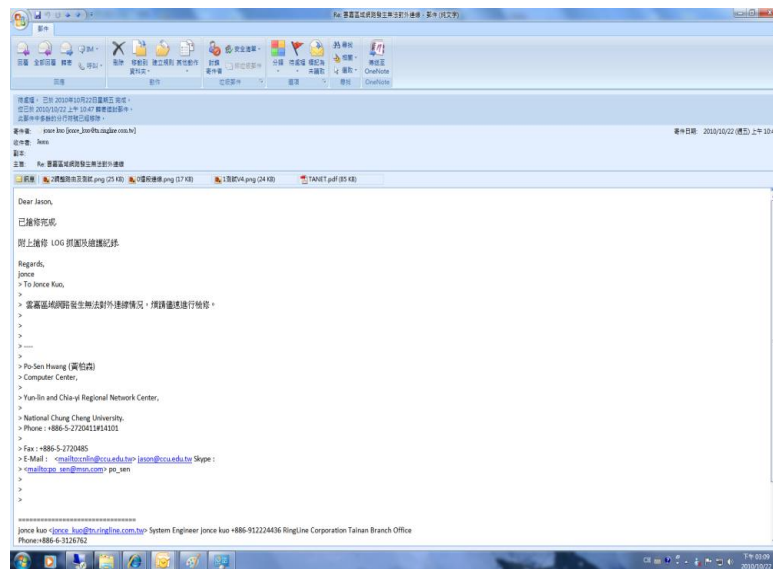


TANet維護廠商遠端連線維修

- 廠商遠端進行維修，將備份於伺服器上之Routing table複製至路由器6509上，並重新啟動系統。
- 廠商檢查系統是否已正常運作？並透過E-mail回報處理狀況及相關記錄。

```
61.222.252.68 - PuTTY
User Access Verification
Password:
TANET_CCU_C6K>en
Password:
TANET_CCU_C6K#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
  Known via "isis", distance 105, metric 20, candidate default path, type level-2
  Redistributing via isis, ospf 123
  Last update from 192.83.196.111 on Vlan10, 4d22h ago
  Routing Descriptor Blocks:
  * 192.83.196.111, from 203.72.43.125, via Vlan10
    Route metric is 20, traffic share count is 1

TANET_CCU_C6K#ping 203.72.43.125
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.72.43.125, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/12/16 ms
TANET_CCU_C6K#
NokiaNetDuet1 putty
Client
```



廠商回報修復記錄

服務紀錄單查詢結果

Page 1 of 1

- 廠商將系統修復後，同時也以電話報告修復狀況，並傳真修復紀錄表。

聯瑞科技股份有限公司											
總機: 24255573 TEL: 02-2651-2441 FAX: 02-2651-2441 傳真: 02-2651-2441	總機: 24255573 TEL: 02-2651-2441 FAX: 02-2651-2441 傳真: 02-2651-2441										
維修服務記錄表 客戶編號: 200401000 單號: 002010094 業務員: worker@ringline.com.tw 客戶編號: 107206											
客戶名稱: _____ 電話: _____ 分機: _____ 聯絡人: _____ 服務地址: <input type="checkbox"/> 現場 <input type="checkbox"/> 工廠 <input type="checkbox"/> 原廠 <input type="checkbox"/> 原廠 <input type="checkbox"/> 原廠 <input type="checkbox"/> 原廠	服務時間: _____ 服務地點: _____ 服務時間: _____ 服務地點: _____										
服務紀錄單內容											
客戶編號: CS10100101 聯絡人: 黃柏森 電子郵件: jason@ccu.edu.tw 問題來源: e-mail 服務類別: 測試 接單編號: _____ 報修時間: 2010/10/22 10:22 問題描述: 配合區網災難復原演練	客戶名稱: 國立中正大學 電話: 05-2720411#14101 服務等級: P3 服務項目: 其他 服務類別: REMOTE SUPPORT 保固期限: _____ 為實工程師: 郭耀榮										
作業說明: 2010/10/22 10:32 郭耀榮 服務等級: P3 狀態: 服務紀錄單已登錄 服務紀錄單登錄成功!! 2010/10/22 10:38 郭耀榮 服務等級: P3 狀態: 工程師處理中 回應客戶登記: 10:15 接獲Email 告知雲嘉區域網路發生無法對外連線情況 10:19 透過Out-Of-Band管理機制連線檢測。 10:20 確定V4對教育館暢通 10:22 聯絡區網確定為演練狀況 10:28 配合調整往嘉義縣網V6路由為2001:288:0:F:123::32 並檢測完成。											
<table border="1"> <thead> <tr> <th>序</th> <th>品名/規格</th> <th>數量</th> <th>序號</th> <th>備註</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>	序	品名/規格	數量	序號	備註						客戶簽名: _____ 工程師簽名: _____ 作業時間: _____
序	品名/規格	數量	序號	備註							

<http://cts.ringline.com.tw/cts/b/RLS1031UC1007/PrintRecord.jsp>

2010/10/22



復原測試

- 代理人員進行網路測試，確認廠商確實已完成修復系統。



事件處理回報

- 代理人員暨區網維運人員向資訊安全官(電算中心李新林主任)回報事件處理狀況。

