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

CCU Computer Center

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員執行復原工作。

CCU Computer Center

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。

CCU Computer Center

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。

CCU Computer Center

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。

CCU Computer Center

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。

CCU Computer Center

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？

CCU Computer Center

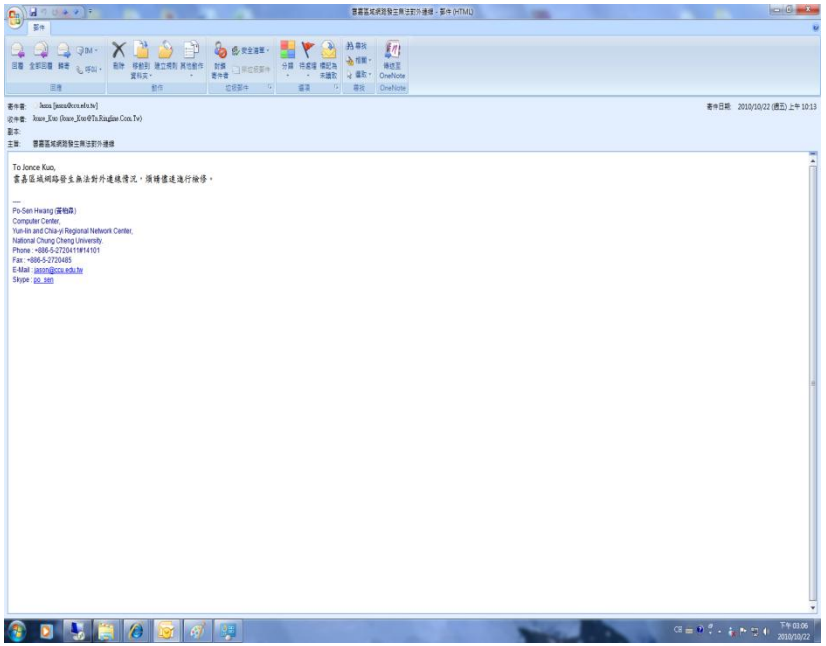
路由器網路狀況檢查

- 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。

CCU Computer Center

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。



CCU Computer Center

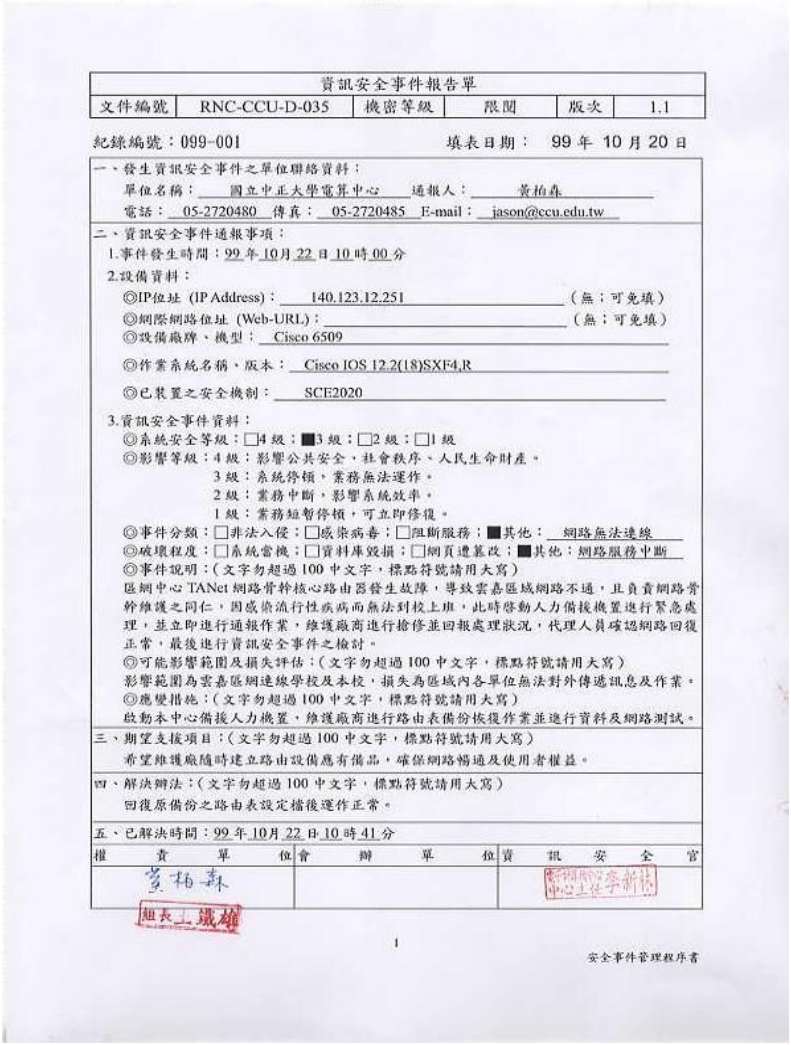
進行資安通報

- 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。

CCU Computer Center

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)SXF4,R
◎已裝置之安全機制：SCE2020

3.資訊安全事件資料：
◎系統安全等級：□4 級；■3 級；□2 級；□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：□非法入侵；□感染病毒；□阻斷服務；■其他：網路無法連線
◎破壞程度：□系統當機；□資料庫毀損；□網頁遭篡改；■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，因感染流行性疾病而無法到校上班，此時啓動人力備援機置進行緊急處理，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，維護廠商進行路由表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	會辦單位	資訊安全官
黃柏森 組長 王識雄		國立中正大學電算中心主任 李新林

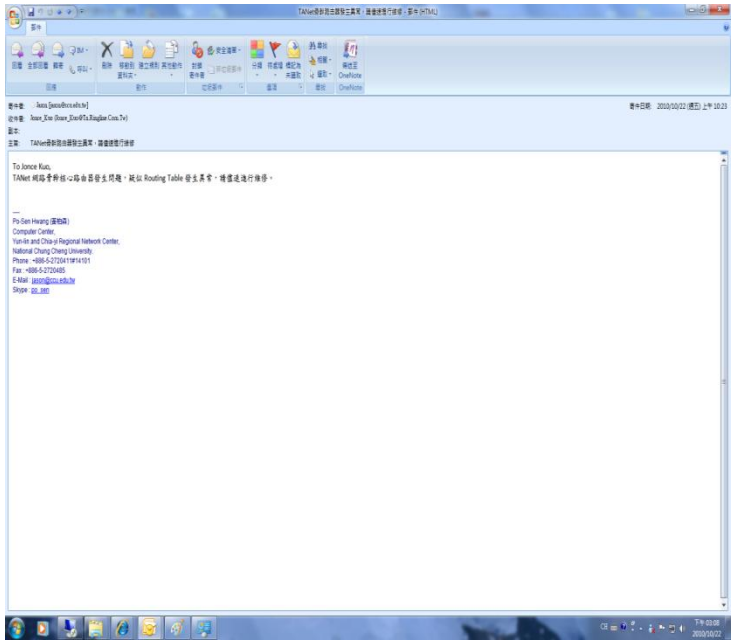
1

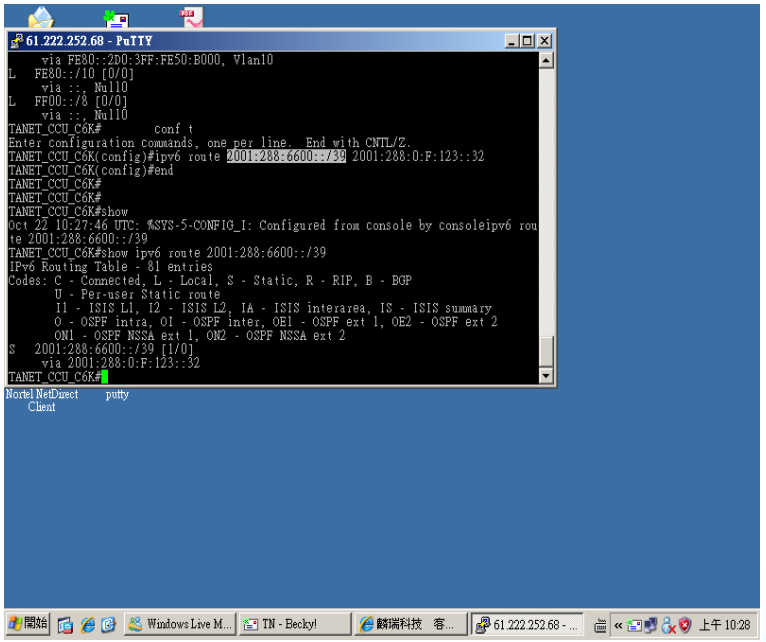
安全事件管理程序書

CCU Computer Center

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。

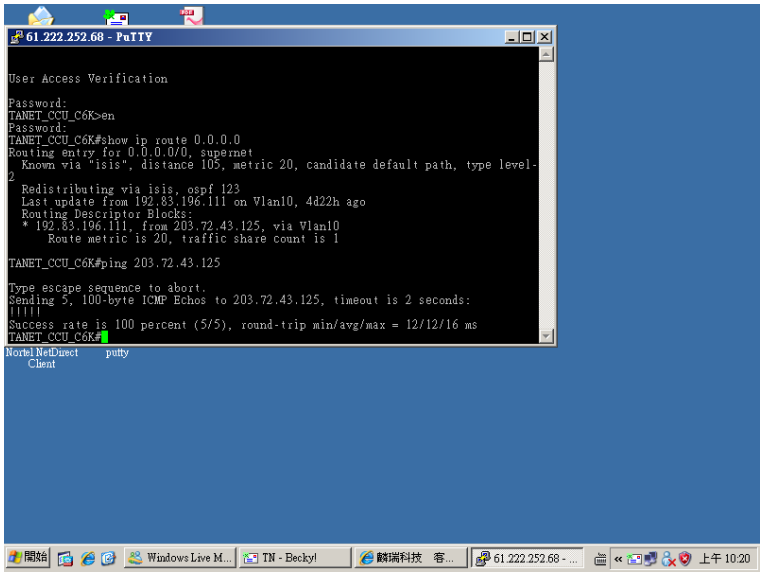


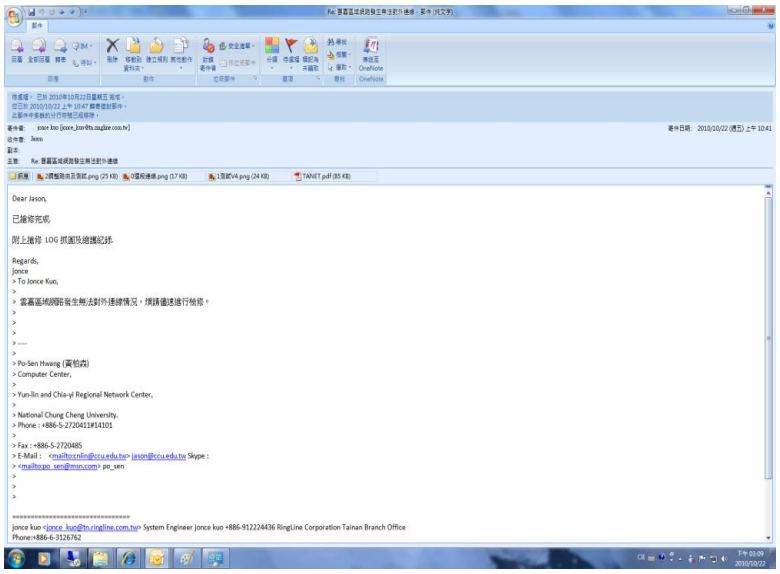


CCU Computer Center

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。

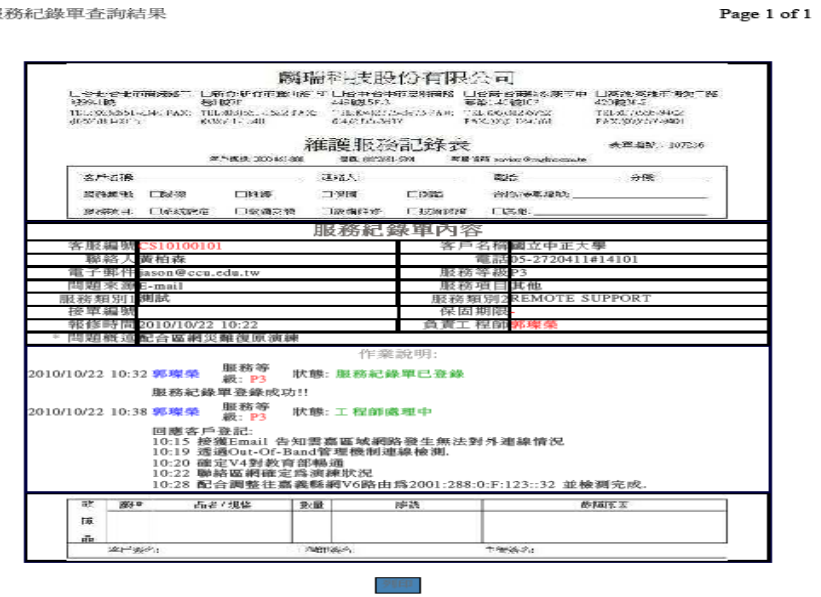




CCU Computer Center

廠商回報修復記錄

- 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。



服務紀錄單查詢結果 Page 1 of 1

麟瑞科技股份有限公司

維護服務記錄表

服務紀錄單內容

客服編號:CS10100101	客戶名稱:國立中正大學
聯絡人:黃柏森	電話:05-2720411#14101
電子郵件:jason@ccu.edu.tw	服務等級:P3
問題來源:e-mail	服務項目:其他
服務類別:測試	服務類別2:REMOTE SUPPORT
接單編號:	保固期限:
報修時間:2010/10/22 10:22	負責工程師:郭璨榮
問題敘述:配合區網災難復原演練	

作業說明:

2010/10/22 10:32 郭璨榮 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 郭璨榮 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 遵循Out-Of-Band管理機制連線檢測.
10:20 確定V4對教育部暢通
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.

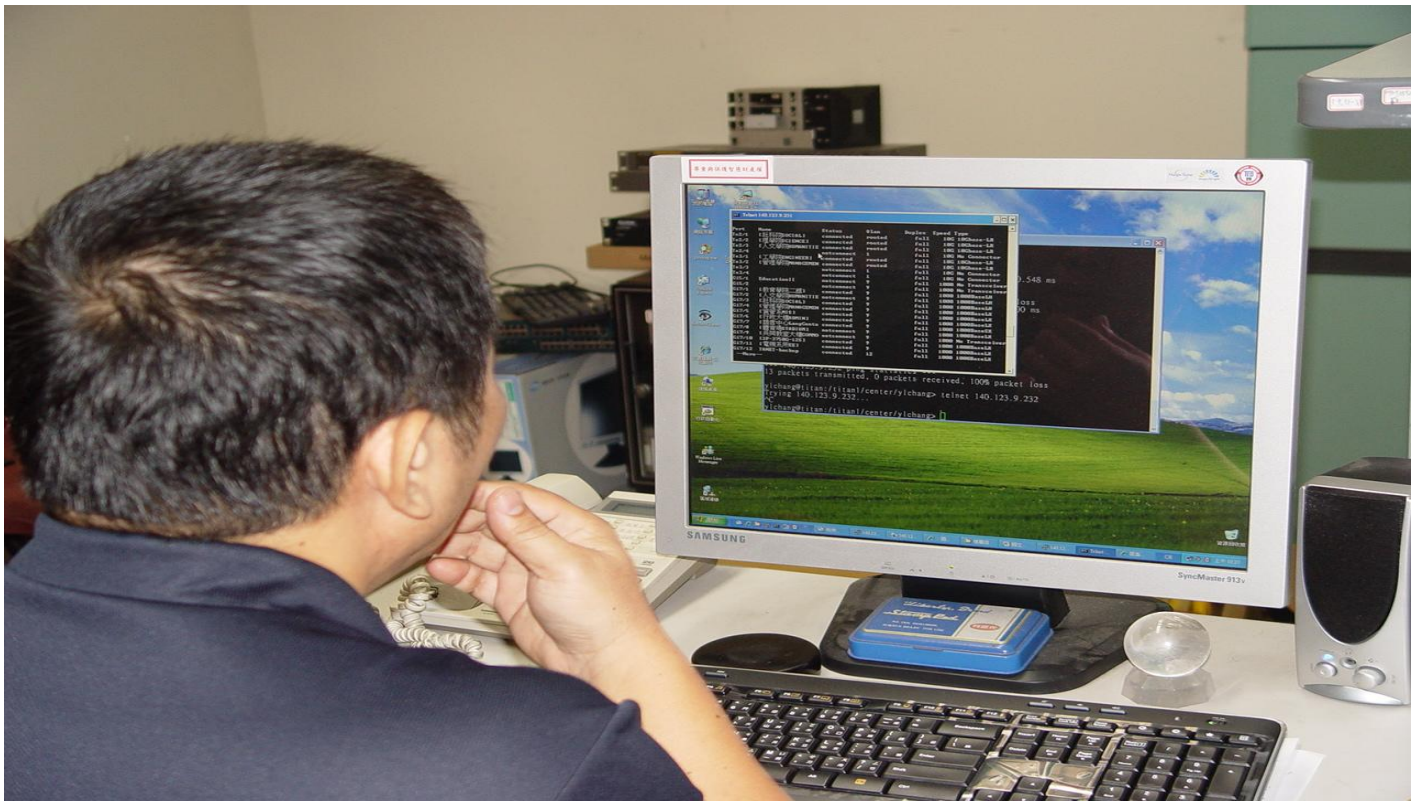
項次	產品編號	品名/規格	數量	序號	故障狀況

http://cts.ringline.com.tw/cts/b/RLS1031UC1007/PrintRecord.jsp 2010/10/22

CCU Computer Center

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。



CCU Computer Center

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。

CCU Computer Center