A Case Study of Integrated Authentication Server in NCNU

張瑛杰 [1]　徐明生 [2]　吳坤熹 [1]
南投區網 [1]　冠閎科技 [2]
{ycc, solomon}@ncnu.edu.tw[1]　anson_hsu@krystal.com.tw[2]

摘要

教育部「TNAet 無線網路漫遊交換中心」提供一個相當具有規模性的認證服務，雖然全國統一以 Radius 作為認證原則，但是各校的執行方式不同，對於管理者和使用者也都產生了不同的問題。因此，我們以國立暨南國際大學整合式認證機制為例，除了解決認證伺服器的備援問題外，還提供兩階段認證的作法，以及單一帳號管理不同使用權的問題，希望能與 TANet 的夥伴分享。

關鍵詞：漫遊，認證，單一帳號登入。

Abstract

Taiwan Academic Network Roaming Center provided a scalable authentication service in Taiwan Academic Network (TANet). Although all TANet users used Remote Authentication Dial-In User Service (RADIUS), the different implements in each school caused the various problems. We take National Chi Nan University as example, discussing the problem of server backup, the two-step authentication and the single sign-on. Hope to share this experience with all server managers in TANet.

Keywords: Authentication, Roaming, Single Sign On.

1. 前言

教育部「TNAet 無線網路漫遊交換中心」的成立，主要是提供各學校與學術相關機關內的認證資訊轉送，藉由各單位內所提供的帳號密碼在跨區域認證時能經由「TNAet 無線網路漫遊交換中心」進行資訊的交換，讓使用者能在不同的無線網路環境下，都能使用單一帳號與密碼進行身分確認。而該計畫最早成立於 2006 年，當時名為「漫遊認證交換中心」，隸屬於資策會及國家高速網路中心無線漫遊服務的單位彼此互連，而後在 2010 年由教育部主導轉型為「TNAet 無線網路漫遊交換中心」。

早期，國立暨南國際大學在初期是隸屬於國家高速網路中心下的漫遊認證交換連線單位，對於該項計畫有相當高的重視，也經常主動通報資策會及國家高速網路中心溝通相關的連線狀況，其中最常發現的認證問題，莫過於校內無線網路認證機制不成熟，以及資策會及國家高速網路中心之間經常發生無法順利交換認證資訊的現象，一來對於管理者造成困擾，二來對於使用者也有諸多不便，但在各單位不斷地努力下，目前教育部「TNAet 全國無線網路漫遊中心」已經能提供一個穩定的認證環境，因此希望能藉由分享國立暨南國際大學校園整合式認證機制提供給 TANet 的夥伴分享，提供給使用者更好的服務品質。

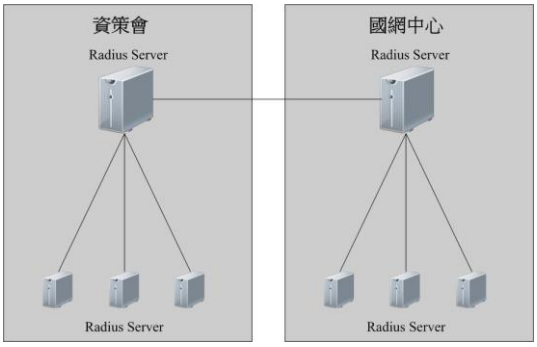

圖 1 早期：漫遊認證交換中心

2. 認證問題

許多學校或單位都有提供無線網路認證的服務，但我們發現，不論是採用閘道式認證與 Thin AP 集中認證方式，通常都會發生一個相同的問題，使用者在使用無線網路服務時，必須經常不斷地執行無線網路認證帳號密碼的輸入動作，主要原因是因為認證時間 Time-Out 了，這樣的困擾若是發生在筆記型電腦的使用者身上，也許只是一件使用感受不佳的體驗，但若發生在智慧型手機的使用者身上，則會變成一件讓人困擾的事情，不論銀幕再怎麼大，要不斷地在智慧型手機上重複地輸入一串帳號和密碼，這樣的使用行為反而變的不太智慧，除此之外，未統一 SSID 的名稱也是另一個降低便利性的主因，其原因在於校內除了有計算機與網路中心所提供的無線網基地台以外，各單位也有可能會自行安裝基地台，如果沒有統一公告的 SSID，就會造成使用者在搜尋與選擇可用的無線網路基地台時的困擾。

由於上述的狀況在許多已經建置無線網路認證機制的單位中都確實存在著，若是不再重視這些已知的困難，只是採購現成的無線網路認證設備，好像已經符合提升安全層級的的需求，但實際上卻變成一種擾民行為。

因此我們期待的是，無線網路認證架構須符合現有無線網路管理架構，在相同 SSID 下提供兩階段

式認證方式，使用者可經由第一層 MAC Address 認證而不需要再進行第二層之 RADIUS 或 LDAP 認證，若第一層認證失敗則自動導向第二層之 Web Captive Portal 網頁認證。

3. 無線網路認證

早期的無線網路的建置方式是將無線網路基地台連線至距離安裝地點最近的網路交換器上，但是這樣的作法會有兩個嚴重的缺點。第一個缺點是因無線網路服務的最後一哩是透過無線電波進行傳輸，如果廣播封包過大會明顯影響網路品質，第二個缺點是因無線網路服務的範圍是一個空間，如果使用者位在兩個不同網段的無線網路基地台之間，漫遊時就必須向 DHCP Server 重新詢問並且取得不同網段的 IP Address，這樣的過程會讓使用者有明顯的斷線感受。因此，為了改善以上的兩個問題，不論是採用閘道式認證與 Thin AP 集中認證方式，我們都建議將無線網路環境已獨立於現有的網路架構外，以實體線路收納作為規劃，請參考圖 2 國立暨南國際大學無線網路拓撲圖，當然也會有些地點的實體線路收納成本過高，就可以善用 Thin AP 的特性作為建置。

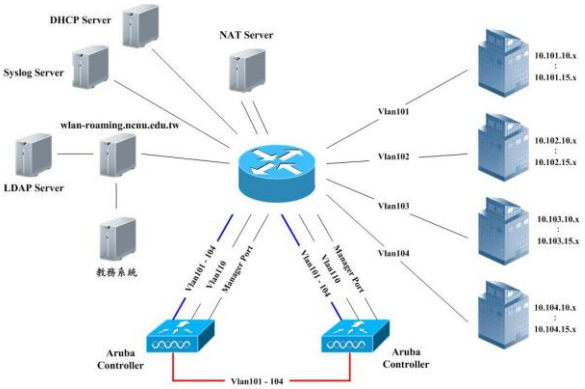

圖 2 國立暨南國際大學無線網路拓撲圖

3.1 註冊網路卡卡號

國立暨南國際大學的無線網路認證服務是提供兩階段式認證方式，第一層 MAC Address 認證，也就是利用 MAC Address 的唯一性，達到一次性認證的作法，因此必須在使用者提供 MAC Address 時就進行身分確認，所以國際暨南國際大學將登錄 MAC Address 的動作與教職員最常使用的教務系統統結合，只要使用者登入教務系統，就可以將各式無線網路設備的 MAC Address 填寫在教務系統上，由於現今智慧型手機與平板電腦的普及，使用者都可以擁有一個以上的無線網路設備，所以提供每個人有 20 組的填寫欄位，同時為了避免填寫錯誤，教務系統提供了填寫時的防呆檢查，MAC Address 是由 0-9 和 A-F 共 12 個字元所組成的，可以減少填寫錯誤發生的機會，請參考圖 3 教務系統 MAC Address 填寫介面。

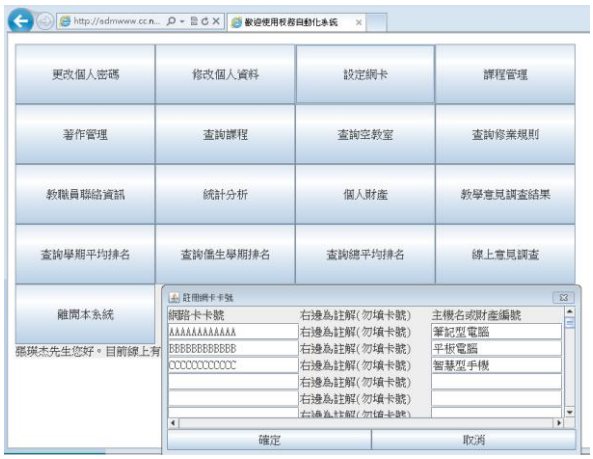

圖 3 教務系統 MAC Address 填寫介面

3.2 E-mail 帳號密碼認證流程

當使用者無法順利通過在第一層 MAC Address 認證時，將自動導向第二層之 Web Captive Portal 網頁認證，請參考圖 4Web Captive Portal 網頁認證介面。在本校使用者尚未將 MAC Address 填寫至教務系統，於連線後首次開啟瀏覽器時將自動被導向認證畫面，只要以本校的 E-mail 帳號密碼就可以順利進行認證動作，如果是來校指導的貴賓所屬的單位有加入 TANet 全國無線網路漫遊計畫，也可以使用貴單位的 E-mail 帳號密碼進行認證，但如果來校指導的貴賓所屬單位沒有加入 TANet 全國無線網路漫遊計畫，本校提供給各系所負責同仁具有建立臨時無線網路漫遊 VIP 帳號的權限，可以提供便利的無線網路使用體驗。

圖 4 Web Captive Portal 網頁認證介面

4. 技術整合

以國立暨南國際大學為例，在無線網路認證架構中使用 Aruba Controller 作為認證伺服器，並且運用 VRRP、Spanning Tree、Radius…等標準協定進行整

合，以下將逐一說明各項設定重點與細節。

4.1 設備再利用率

各校在導入無線網路認證服務之前，大多數已建置各式不同廠牌的無線網路基地台，為了強調現有設備的再利用率，在規劃無線網路認證架構須符合現有無線網路管理架構。

以國立暨南大學為例，在導入無線網路認證服務之前，既有的無線網路基地台包括：Cisco、D-LINK 和 Ruckus…等廠牌多種廠牌，若採購只支援 Thin AP 的無線網路認證伺服器則必須全部汰換約 160 台的無線網路基地台，除了建置初期投入成本過高外，現有設備也都還不到達汰換階段；若採購只支援閘道式的無線網路認證伺服器，在不適合實體線路收納廣闊的校園或具有第二校區的學校則無法順利地集中管理，造成資安漏洞，考慮以上的問題，選擇可整合現有無線網路管理架構的認證方式，才能提升設備的再使用率。

4.2 VRRP

在規劃網路架構時經常發生的錯誤就是忽略了備援機制，在無線網路認證架構中，若是沒有考慮備援機制，就會發生 Single Point of Failure 的嚴重問題，也就是當網路設備發生故障時，整體網路就會斷線停止服務，例如：閘道式認證架構，就會因為認證伺服器故障而斷成實體線路中斷；若是 Thin AP 集中式認證架構，就會發生無法管控所有的 Thin AP，造成無法提供正常服務。對此，我們的做法是採購兩台 Controller 提供備援機制，並且透過 VRRP(Virtual Router Redundancy Protocol)讓兩台 Controller 在管理上具備 HA(High availability)的能力，避免 Single Point of Failure 的狀況。

4.3 Spanning Tree

接下來要討論的，是如何善用 Spanning Tree 在 HA 架構下進行負載平衡(Load Balance)。雖然目前的 HA(High availability)架構僅有 Master-Local 的方式，也就是說主控權在 Master Server 上，但是我們運用 Spanning Tree 的方式，將全校四個無線網路網段 Vlan101-Vlan104 以優先權的設定 Forwarding 與 Block(請參考圖 5 Spanning Tree Vlan101 和圖 6 Spanning Tree Vlan102)，例如：Vlan101 和 Vlan103 的優先權設定在 Master Controller 上，而 Vlan102 和 Vlan104 的優先權設定在 Local Controller 上(請參考表 1 Spanning Tree Vlan101，103 和表 2 Spanning Tree Vlan102，104)，也就是說在 VRRP 的架構下，如果有其中一台設備故障，將由正常運作的 Controller 接手所有的服務，包括管理權與四個網段的流量。

除此之外，經由 Spanning Tree 的設定，讓無線網路的流量分攤在兩台 Controller 時，對於進行認證過程所造成的 CPU Loading 也就各自落在不同的 Controller 上，經由 Spanning Tree 的設定，可以避免 Master-Local 架構上總有一台設備呈現閒置狀態的缺點。

```
VLAN0101
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     0003.31e4.2c65
              This bridge is the root
              Hello Time   2 sec  Max Age  6 sec  Forward Delay  4 sec

  Bridge ID   Priority    32768
              Address     0003.31e4.2c65
              Hello Time   2 sec  Max Age  6 sec  Forward Delay  4 sec
              Aging Time 300

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi2/1               Desg FWD 19        128.129  P2p
Gi2/5               Desg FWD 4          16.133  P2p
Gi2/7               Back BLK 4         128.135  P2p
```

圖 5 Spanning Tree Vlan101

```
VLAN0102
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     0003.31e4.2c66
              This bridge is the root
              Hello Time   2 sec  Max Age  6 sec  Forward Delay  4 sec

  Bridge ID   Priority    32768
              Address     0003.31e4.2c66
              Hello Time   2 sec  Max Age  6 sec  Forward Delay  4 sec
              Aging Time 300

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi2/2               Desg FWD 4         128.130  P2p
Gi2/5               Back BLK 4         128.133  P2p
Gi2/7               Desg FWD 4          16.135  P2p
```

圖 6 Spanning Tree Vlan102

表 1 Spanning Tree Vlan101，103

```
Core#show run int gi2/5
Building configuration...

Current configuration : 193 bytes
!
interface GigabitEthernet2/5
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 101-104
 switchport mode trunk
 spanning-tree vlan 101,103 port-priority 16
end
```

表 2 Spanning Tree Vlan102，104

```
Core#show run int gi2/7
Building configuration...

Current configuration : 193 bytes
!
interface GigabitEthernet2/7
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 101-104
 switchport mode trunk
 spanning-tree vlan 102,104 port-priority 16
end
```

收斂時間過久其實是 Spanning Tree 一直存在的的問題，對此我們提出一個簡單的解決辦法，就是縮短 Hello Time 的時間，詳細指令請參考表 3 Spanning Tree Hello Time。以本校的設定為例，將 Hello Time 縮短為 2 秒，並且進行時實際測試，把其中一台 Controller 的電源線拔除，切換過程僅僅掉了一個封包，而後將電源線接回 Controller 時，則是完全沒有封包遺失的狀況，所以若是真的發生了設備故障的狀況或必須停機維護時，也完全不影響使用者的網路使用情況，是一個穩定度與備援性相當高的設計架構。

表 3 Spanning Tree Hello Time

```
Core(config)#spanning-tree vlan 101 hello-time 2

<1-10>    number of seconds between generation of
config BPDUs
```

4.4 Freeradius

為了能提供整合性的認證方式，我們架設了一台 Radius Server：wlan-roaming.ncnu.edu.tw，建置在 1U IBM x336 機架型的伺服器上，僅提供了 4G 的記憶體，作業系統為 CentOS 5.5 32 位元作業系統，透過 yum install freeradius2.i386 安裝 Radius 服務 (請參考表 4 安裝 Freeradius2.i386)，經過效能測試證明，不需要高檔的伺服器就可以提供具有整合性的服務。

表 4 安裝 Freeradius2.i386

```
[root@wlan-roaming ~]# yum install
freeradius2.i386

Freeradius2.i386 : High-performance and highly
configurable free RADIUS server
```

wlan-roaming.ncnu.edu.tw 提供了多項的服務內容，主要負責與執行的流程(請參考圖 7 認證流程)如下：

1. 國立暨南國際大學與 TNAet 無線網路漫遊交換中心所介接的 Radius Server。讓本校的教職員與學生能在其他已加入無線網路漫遊的單位，能夠使用本校的 E-mail 帳號進行 Web Captive Portal 網頁認證，並且提供參訪的貴賓能夠使用已加入 TANet 無線網路漫遊的帳號密碼進行 Web Captive Portal 網頁認證。
2. 本校使用者在校內進行 Web Captive Portal 網頁認證時的 Radius Server。每當使用者進行 Web Captive Portal 網頁認證時，wlan-roaming.ncnu.edu.tw 會將使用者的帳號密碼傳送至後端的 LDAP Server 進行身份確認。
3. 使用者進行 MAC Address 認證時的 Radius Server。我們撰寫了一個資料擷取程式執行於 Radius Server 上，每隔十五分鐘會主動向本校的教務系統詢問使用者與註冊的 MAC Address，快速地進行資訊更新，並且該程式提供防呆功能，如果教務系統無法存取資料時，會由最後一次擷取的資料作為最新資料，同時通知管理者進行查看，表 5 為 Radius 設定檔中加入 MAC Address 的設定方式。
4. 用於允許校內特定使用者可使用自己的 E-mail 帳號密碼，登入本校無線網路漫遊 VIP 帳號的建立網頁，如果參訪貴賓沒有 TANet 無線網路漫遊帳號時，各單位的負責同仁可以快速地提供臨時無線網路 VIP 帳號密碼的方式，也就是所謂的 Single Sign On 功能。

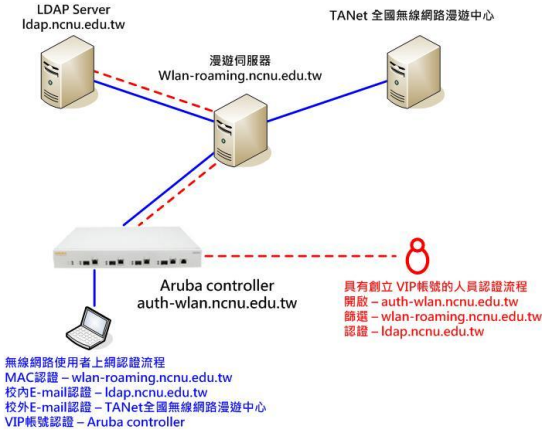

圖 7 認證流程

表 5 MAC Address 設定方式

```
設定檔案位置
[root@wlan-roaming ~]# vi /etc/raddb/users

設定範例
"A 網路卡號" Cleartext-Password := "A 網路卡號"
"B 網路卡號" Cleartext-Password := "B 網路卡號"
"C 網路卡號" Cleartext-Password := "C 網路卡號"
```

2011 年 8 月 5 日 wlan-roaming.ncnu.edu.tw 由

教務系統上單一次統計的 MAC Address 已經超過了一萬多筆，整體 Radius 系統運作上呈現正常狀態，請參考表 6 MAC Address 註冊數量統計。

表 6 MAC Address 註冊數量統計

```
[root@wlan-roaming ~]# date
五　 8 月  19 14:34:31 CST 2011
[root@wlan-roaming ~]# wc -l /etc/raddb/users
10815 /etc/raddb/users
```

4.5 Single Sign On

現今網路服務項目越來越多，使用者的困擾就是必須記住越來越多組的登入帳號密碼，若一有遺失則必須重新申請，費時又費力，因此 Single Sign On 就變得格外重要。以國立暨南國際大學為例，在無線網路認證服務中，結合 Single Sign On 的概念，我們授權特定使用者能建立臨時無線網路 VIP 帳號，以下以作者張瑛杰的 E-mail 帳號 ycc@ncnu.edu.tw 為例進行說明。

假設管理者要授權給張瑛杰同仁具有校內臨時使用的無線網路漫遊 VIP 帳號的建立權限，則管理者只需要在 wlan-roaming.ncnu.edu.tw 的 Radius 的 users 設定檔中新增「帳號」和「類別」，因為 Aruba Controller 發現登入的帳號並非管理者帳號時，會將登入的帳號和密碼送往 wlan-roaming.ncnu.edu.tw 進行帳號的篩選，如果在 wlan-roaming.ncnu.edu.tw 上有帳號，類別為 Aruba-Admin-Role = "guest-provisioning"時並且通過後端 LDAP Server 的認證時，Aruba Controller 會將該名使用者導向建立校內臨時使用的無線網路漫遊 VIP 帳號的網頁上。

其中，由於資訊安全的因素，管理者帳號獨立建立於 Controller 上，但基於 Single Sign On 的考量，對於管理者與被授權者都是使用相同的 Web Captive Portal(請參考圖 8 Web Captive Portal：管理者與被授權者)，可以減少額外建置 Web Captive Portal 的需求。

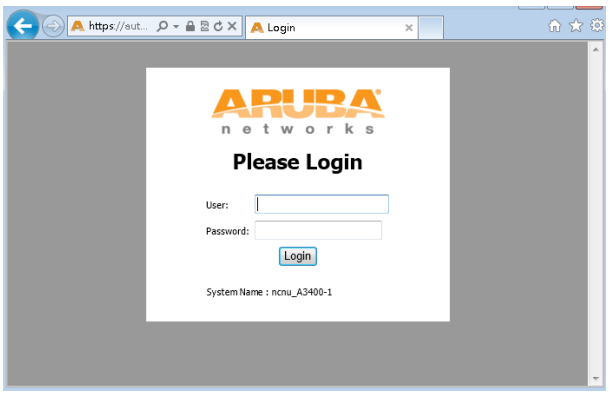

圖 8 Web Captive Portal：管理者與被授權者

經由以上的規劃，一般使用者或被授權者，都只需要記住一組 E-mail 帳號密碼就可以在無線網路漫遊認證的環境中都暢行無阻；被授權者與管理都經由相同的 Web Captive Portal 執行不同的管理權限。

表 7 Aruba-Admin-Role 設定方式

```
設定檔案位置
[root@wlan-roaming ~]# vi /etc/raddb/users

設定範例：
帳號    Cleartext-Password :=    ""
        Aruba-Admin-Role = "類別"

實際範例：
ycc     Cleartext-Password :=    ""
        Aruba-Admin-Role = "guest-provisioning"
```

```
[root@proxy3 ~]# radtest E-mail帳號 E-mail密碼 RadiusServerIPAddress 0 確認碼
Sending Access-Request of id 185 to RadiusServerIPAddress port 1812
        User-Name = "E-mail帳號"
        User-Password = "E-mail密碼"
        NAS-IP-Address = RadiusServerIPAddress
        NAS-Port = 0
rad_recv: Access-Accept packet from host RadiusServerIPAddress port 1812, id=18
5, length=46
        Aruba-Admin-Role = "guest-provisioning"
```

圖 9 Aruba-Admin-Role 測試結果

4.6 認證測試

對於國立暨南國際大學無線網路認證架構，進行了實際運作測試，我們提供以下的測試內容與數據進行說明：

測試日期：2011/05/29
- 上午 09:55 啟動認證功能
- 早上 10:00 啟動 CPU Loading 統計
- 早上 10:40 啟動 User 統計
- 中午 12:10 拔掉 Local Aruba Controller 電源
- 下午 01:25 接回 Local Aruba Controller 電源
- 下午 02:20 結束測試時間

每隔 5 分鐘統計 1 次數據：
CPU-1：Master Controller CPU Loading (單位 %)
CPU-2：Local Controller CPU Loading (單位 %)
請參考圖 10 Controller CPU Loading

每隔 5 分鐘統計 1 次數據：
USER-1：Master Controller 的認證成功 User 人數
USER-2：Local Controller 的認證成功 User 人數
請參考圖 11 認證成功使用者數量統計

測試結果說明：

1. 當使用者進行認證時會使 Controller CPU

Loading 有短暫升高現象。

2. 若是沒有使用者進行認證時，Controller CPU Loading 有機會降至為 0。
3. 當 Local Controller 無法提供正常服務時，Master Controler 會接手所有的服務，因此 Master Controller CPU Loading 會有短暫升高的現象，但隨著認證過程的結束，Controller CPU Loading 有機會降至為 0。
4. 當斷線的 Local Controller 恢復連線時，兩台 Controller 的 CPU Loading 都有短暫升高的現象。
5. 測得單台最高 Controller CPU Loading 為 18%
6. 本次測得總計最高認證成功 USER 數為 268 人
7. 於全校四個無線網路網段 Vlan101-Vlan104 進行實際認證測試，包括 MAC Address 和 Web Captive Portal 網頁認證，都沒有發生認證上的問題。

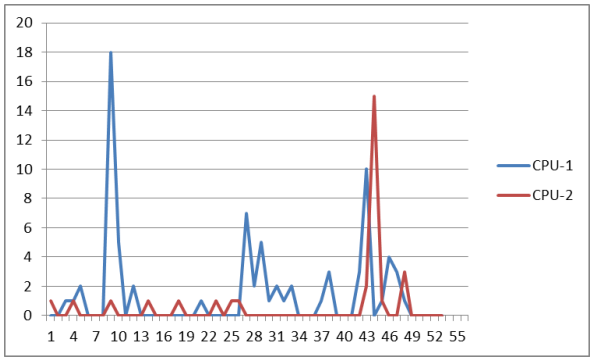

圖 10 CPU 使用率

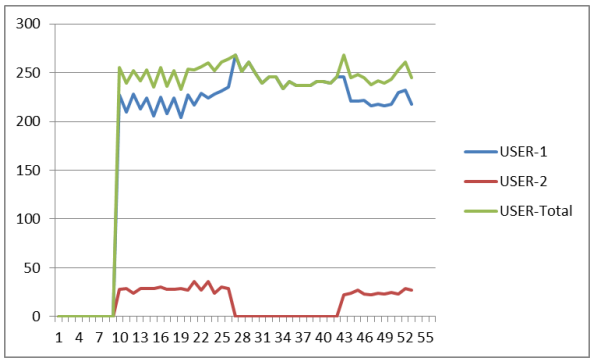

圖 11 認證成功使用者數量統計

使用者反應：

1. 本日值班的圖書館同仁表示，有些同學不知道自己的 E-mail 的帳號和密碼，所以無法進行認證。

測試心得：

1. 依據實際的使用人數與 CPU Loading 的測試數據表示，目前的架構是足以提供正常的認證服務與使用品質。
2. 需要多舉辦推廣講座，並針對如何查詢網卡、認證方式說明以及創立 VIP 帳號的流程作為重點項目。
3. 如果要將目前的架構運用於有線網路的環境下，也是一個相當完整的方式。

5. 結論

TNAet 無線網路漫遊是一個相當便利的服務，但是對於校內的管理者而言，要考慮降低造成使用不便的狀況下，才順利地導入這一個資訊安全的議題，是一個相當嚴苛的挑戰。

因此，在國際暨南大學的建置經驗中，是在相同 SSID 下提供兩階段式認證方式，使用者可經由第一層 MAC Address 認證而不需要再進行第二層之 RADIUS 或 LDAP 認證，若第一層認證失敗則自動導向第二層之 Web Captive Portal 網頁認證，並且結合 Single Sign On 的概念讓被授權的同仁可以使用同一組帳號密碼登入建立臨時無線網路漫遊 VIP 帳號密碼的網頁，期望能將以上經驗與 TANet 的夥伴分享。

參考文獻

[1] Aruba, http://www.arubanetworks.com/
[2] Freeradius, http://freeradius.org/.
[3] Radius, http://www.ietf.org/rfc/rfc2865.txt
[4] RSTP, http://www.ietf.org/rfc/rfc4318.txt
[5] VRRP, http://www.ietf.org/rfc/rfc2338.txt
[6] VRRP, http://www.ietf.org/rfc/rfc3768.txt
[7] 冠閎資訊股份有限公司, http://www.krystal.com.tw/
[8] 國立暨南國際大學無線網路漫遊中心 http://wlan-roaming.ncnu.edu.tw