臺中市市立學校無線網路 Local Bridge Mode 服務　2017/3 修訂

一、適用範圍

本市市立學校無線網路系統為 Aruba 無線基地台（Thin AP）且中央控制器（controller）由教育局設備擔任。

二、建置目的

原無線系統提供 tc 及 tc-802.1x 兩 SSID，認證通過後因 IP 由教育局統一分配，因此視同為校外使用者，無法取用校內的特定應用服務（如校內提供之印表機、網路磁碟機、視訊教學..）。學校提出申請本項服務執行後，會以學校 tc-[Domain Name] 新增 SSID，學校校內教職員生連線此 SSID 認證成功後，IP 將由校內提供，故可取用校內限制使用的特定應用服務，提供校內教職員生進行校內行動學習之需求。

臺中市市立學校無線網路 SSID 表列

SSID	TANetRoaming	tc-802.1x	tc-[學校 Domain]	tc-[學校 Domain]-mac
無線協定	無	WPA2-Enterprise	WPA2-Enterprise	WPA2-PSK
加密方式	無	WPA2/AES	WPA2/AES	WPA2/AES
認證協定	Web 認證	802.1X (PEAPv1/EAP-GTC)	802.1X (PEAPv1/EAP-GTC)	MAC address
後端認證主機	RADIUS Server	LDAP Server	RADIUS/LDAP/AD Server	RADIUS Server
IP 發放單位	資網中心	資網中心	本地端學校	本地端學校
使用對象	臨時訪客、跨區漫遊、臺中市市立各級學校教職員	臨時訪客、跨區漫遊、臺中市市立各級學校教職員	校內使用者	校內行動裝置
安控方式	校內網路無存取權，僅提供上網服務	校內網路無存取權，僅提供上網服務	可存取校內網路，並提供上網服務	可存取校內網路，並提供上網服務

三、學校端配合事項

1. 因認證成功後 IP 由校內提供，故建議學校在 Aruba AP 所在網段提供 **DHCP** 服務，方便行動裝置認證通過後**自動取得 IP**，進行網路存取。
2. 若學校規劃行動裝置取得 IP 為 Private IP，請學校端自行設置好 NAT 服務。
3. 因 IP 由校內提供，建議建置流量紀錄設備(Netflow、FortiAnalyzer..)，方便未來若發生資安事件之追踪。
4. 學校端 DHCP 服務可分配的 IP 數量請考量學校內同時連線的行動裝置數量。

四、服務方案

目前規畫下列 Local Bridge Mode 服務方案由學校自行考量後選擇合適方案進行建置，未提出申請之學校則維持現狀不改變。

方案 1. 登入所需帳號密碼認證由教育局提供及維護

- 帳號密碼為「教育局公務帳號」。
- 外校教職員生無法使用。
- 學校需至「教育局首頁」「7.公務作業」「7-1.公務作業專區」「7-1-2.公務帳號管理」「單位人員管理」定期維護各校校內之人員名單。

方案 2. 登入所需帳號密碼認證由學校提供及維護

- 由學校全權決定哪些使用者可以使用無線網路 Local Bridge Mode 服務。
- 學校需提供認證服務 （RADIUS server、LDAP server 或 Windows AD）。

方案 3. 利用設備 MAC Address 認證

- 由學校全權決定哪些行動裝置可以使用無線網路 Local Bridge Mode 服務。
- 學校需建置 RADIUS server 擔任認證服務，並自行定期維護允許使用之 MAC Address 清單（可參考附件自行架設）。

五、資訊安全之考量

當可以利用無線網路存取校內特定服務，便有可能為駭客提供另一攻擊之路徑。故在申請本項服務前，請各校務必考慮開啟本項服務後對於校內資訊安全之衝擊，並完成相關資訊安全防護建置（例如調整防火牆、訂定密碼管理規則、學務系統使用 https 傳送及使用自然人憑證登入..）。

六、行動裝置連線設定

1. Local Bridge Mode 採用的認證及傳送規範與 SSID：tc-802.1x 相同，因此設定時請參考 tc-802.1x 的設定方式設定（設定方法相同僅 SSID 不同）。
2. 因 Windows 系統未內建認證所需的 PEAP-GTC Plug-In 元件，若未安裝則需先至 SSID： tc 登入畫面中下載並安裝。Windows EAP-GTC 元件目前提供 Windows XP、Windows Vista 、Windows 7/8、Windwos 10（32/64 位元）等作業系統。
3. 大部分 Android 裝置及所有的 Apple iOS 裝置已內建認證所需的元件，不用額外再安裝。

七、附件：Free RADIUS server 架設

Free RADIUS server 架設　　2017/3 編修

一、本範例以 CentOS6 為主來示範安裝 FreeRADIUS，其他 OS 請自行參考調整。

```
#yum install freeradius*
```

安裝後設定檔預設會放在 /etc/raddb 之下

二、修改設定檔

1. 修改 clients.conf

```
#vi /etc/raddb/clients.conf
```

在檔案最後加入允許查詢的教網中心 controller IP(設定前請與資網中心網路組連絡，確認 AP 使用之 controller IP，目前為 163.17.38.208、163.17.38.209、120.109.231.253、120.109.239.253 四台)

```
client 163.17.38.208 {
                secret = xxxxxx
        }
client 163.17.38.208 {
                secret = xxxxxx
        }
client 120.109.231.253 {
                secret= xxxxxx
          }
client 120.109.239.253 {
                secret= xxxxxx
          }
```

※secret=xxxxx 請自訂

2. 修改 proxy.conf

```
#vi /etc/raddb/proxy.conf
```

確認 DEFAULT 段內容為下

```
realm DEFAULT {
        type                = radius
        authhost            = LOCAL
        accthost            = LOCAL
}
```

3. 啟動 radiusd 並設為開機啟動

```
#service radiusd restart
#chkconfig radiusd on
```

※CentOS 7 請使用

#/bin/systemctl restart radiusd.service

三、本機防火牆及學校防火牆加入允許來源為教網中心 controller IP 查詢的規則

1. 本機：

```
#vi /etc/sysconfig/iptables
```

加入

-A INPUT -s 163.17.38.208 -p udp --dport 1812:1814 -j ACCEPT

-A INPUT -s 163.17.38.209 -p udp --dport 1812:1814 -j ACCEPT

-A INPUT -s 120.109.231.253 -p udp --dport 1812:1814 -j ACCEPT

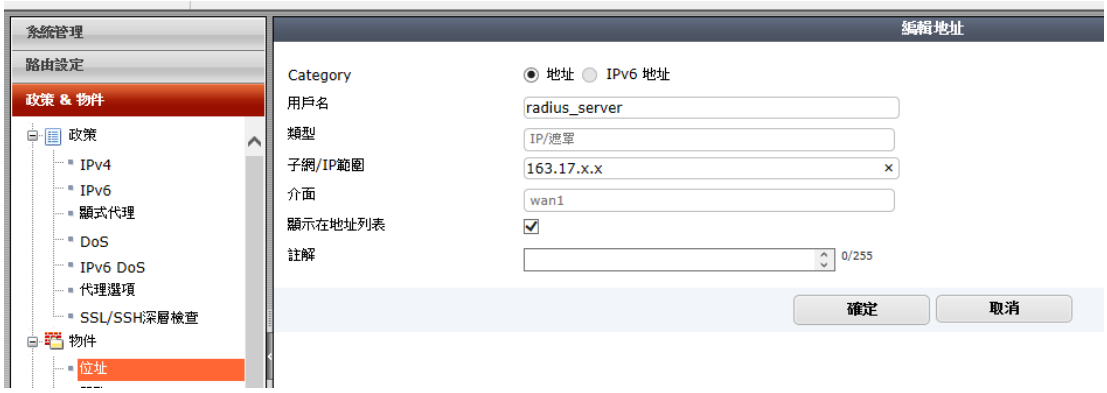
-A INPUT -s 120.109.239.253 -p udp --dport 1812:1814 -j ACCEPT

重新啟動 iptables

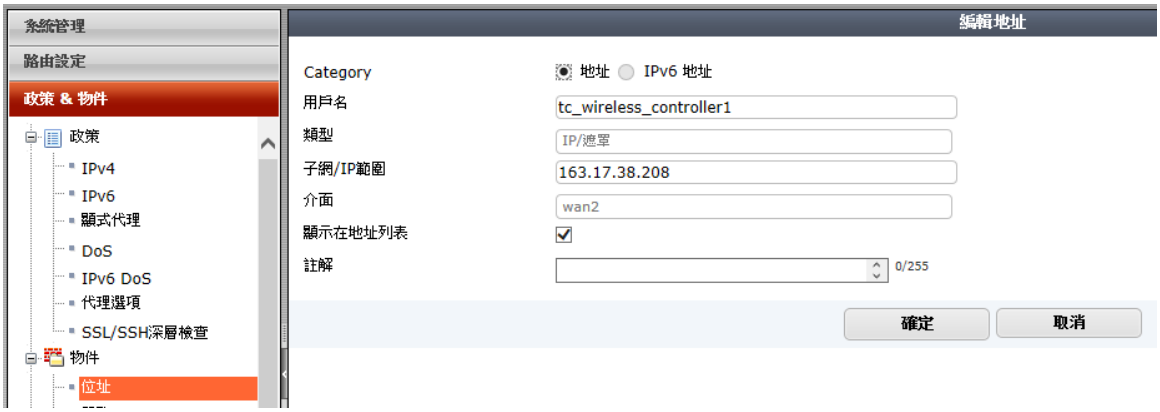
```
#service iptables restart
```

2. 學校防火牆 下面以 FG200D 示範。

2-1 自訂學校架設之 radius server 位址



2-2 加入資網中心無線控制器 IP



※請加入 資網中心目前 4 部無線控制器 IP

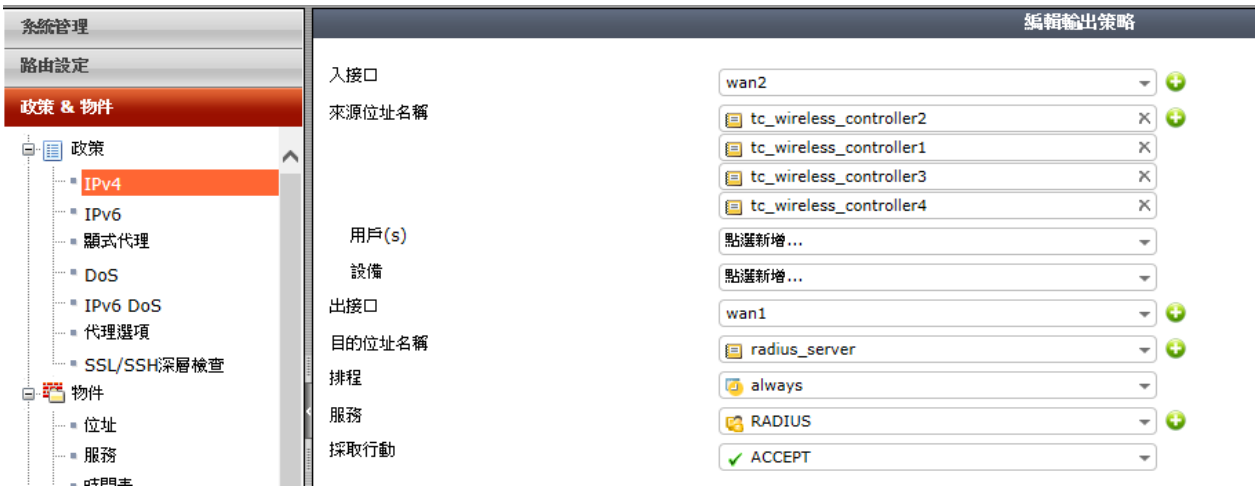
163.17.38.208

163.17.38.209

120.109.231.253

120.109.239.253

2-2 外對內加入防火牆規則(請按照學校實際對外對內之介面設定)



四、加入允許之行動裝置 MAC Address

#vi /etc/raddb/users

請將收集到的 MAC Address 依下面格式加入 users 檔(英文字母要大寫)

00000000000A Auth-Type := Local, User-Password := "00000000000A"

00000000000B Auth-Type := Local, User-Password := "00000000000B"

00000000000C Auth-Type := Local, User-Password := "00000000000C"

※若為 CentOS7 freeradiusd 3.x 格式為

00000000000A Cleartext-Password := "00000000000A"

修改內容後需重新啟動 radiusd

```
#service radiusd restart
```

五、測試

```
#radtest 00000000000A 00000000000A 127.0.0.1 0 testing123
```

```
Sending Access-Request of id 131 to 127.0.0.1 port 1812
        User-Name = "00000000000A"
        User-Password = "00000000000A"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 0
        Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=131, length=20
```

有回應 Access-Accept 就是沒問題了。