

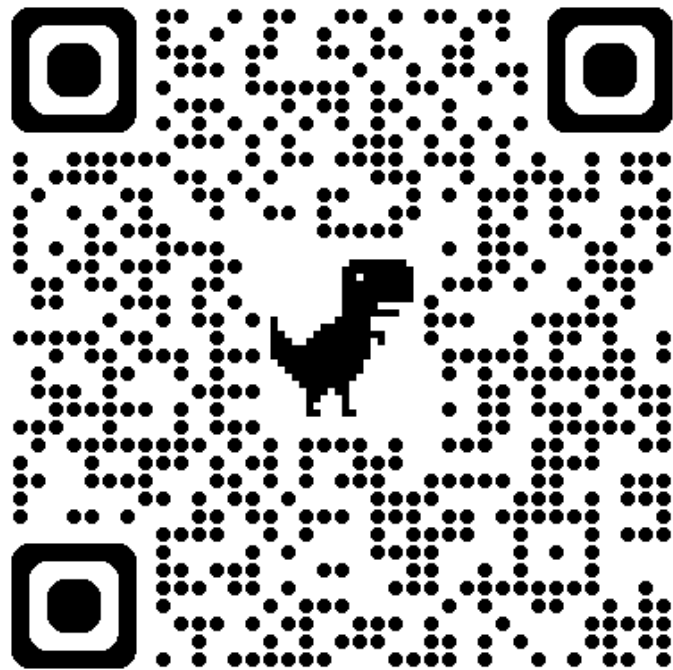
淺談 eduroam

SITCON 2025 Lightning Talk

本次簡報 設定檔下載

<https://edur.isli.me/>

本次提到的所有內容都可以在裡面找到
之後可以打右下角的網址



whoami;



chilin.h / 麒麟

國立鳳新高中 學生
ICEDTEA CTF 戰隊維運
研究範圍：網路安全



Eric / e0pwr

國立東華大學 學生
研究範圍：網路安全

eduroam

- 歐盟 GÉANT 主導
 - <https://eduroam.org/>
 - 跨國 WiFi 身分認證系統
 - 以教育機構為主
- 臺灣主管機關
 - TANet 漫遊認證交換中心
- TL;DR:
讓你能在國內外連網路的東西



以教育雲帳號連線 eduroam 操作說明手冊

eduroam 國際漫遊簡介

學術說法：eduroam(education roaming)是一個為建立國際教育及科研機構間無線區域網路漫遊體系的計畫，意在推動全球教育及科研單位之間的無線區域網路服務共享。

簡單來說：到各教育單位研習時，如果有 eduroam 的無線訊號就可以用教育雲帳號認證設定過後上網，一組帳號可輸入多項個人設備，連線有加密比較安全。



連eduroam

從來不覺得~~玩樂團~~開心過

國外的解法？



- <https://cat.eduroam.org/>
- 設定檔資料庫
 - 歐盟 GÉANT 管理
 - 各國透過各國主管單位上傳
 - 台灣不知道為什麼沒有
- 設定檔
 - 副檔名 .eap-config
 - xml 格式
 - 可以自己寫
 - 配套軟體：geteduroam

The screenshot shows the eduroam website's configuration assistant tool. At the top, there's a navigation bar with links: Start page, About, Language, Help, Manage, and Terms of use. Below the navigation bar, the main heading is "eduroam Configuration Assistant Tool". The central part of the page features a large image of people using mobile devices, with text overlays: "eduroam® installation made easy:", "Apple iOS devices", "iPhone, iPad, iPod touch", "Custom built for your organisation", and "Digitally signed by the organisation that coordinates eduroam®: GÉANT Association". On the right side of this image, there's a small inset showing a mobile screen with an "Install Profile" dialog box for "eduroam University of Samoklevo". Below the main image, the text reads "Welcome to eduroam CAT" and "Connect your device to eduroam®". A paragraph states "eduroam® provides access to thousands of Wi-Fi hotspots around the world, free of charge. [Learn more](#)". At the bottom, there's a large blue button that says "Click here to download your eduroam® installer".

eduroam

- 寫了 Template

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <EAPIdentityProviderList xmlns:xsi="http://www.w3.org/2001/XMLSchema-inst
3   <EAPIdentityProvider version="1" lang="en" ID="#Realm#" namespace="urn
4     <AuthenticationMethods>
5       <AuthenticationMethod>
6         <EAPMethod>
7           <Type>25</Type>
8         </EAPMethod>
9         <ServerSideCredential>
10           <CA format="X.509" encoding="base64">#PEAP_MSCHAPv2Cent#</CA>
11           <ServerID>#Domain#</ServerID>
12         </ServerSideCredential>
13         <ClientSideCredential>
14           <OuterIdentity>anonymous@#Realm#</OuterIdentity>
15           <InnerIdentitySuffix>#Realm#</InnerIdentitySuffix>
16           <InnerIdentityHint>true</InnerIdentityHint>
17         </ClientSideCredential>
18         <InnerAuthenticationMethod>
19           <EAPMethod>
20             <Type>26</Type>
21           </EAPMethod>
22         </InnerAuthenticationMethod>
23       </AuthenticationMethod>
24     </AuthenticationMethod>
```

eduroam

- 工人智慧找了台灣各大學 Realm

```
127 anonymous@tpcu.edu.tw
128 anonymous@ttcs.edu.tw
129 anonymous@ttu.edu.tw
130 anonymous@ntou.edu.tw
131 anonymous@o365.mitust.edu.tw
132 anonymous@tut.edu.tw
133 anonymous@uch.edu.tw
134 anonymous@usc.edu.tw
135 anonymous@utaipai.edu.tw
136 anonymous@vnu.edu.tw
137 anonymous@ms.wfu.edu.tw
138 anonymous@mail.wtuc.edu.tw
139 anonymous@mail.ypu.edu.tw
140 anonymous@stu.mail.ypu.edu.tw
141 anonymous@mail.yzu.edu.tw
142 anonymous@chc.edu.tw
143 anonymous@cy.edu.tw
144 anonymous@hcc.edu.tw
145 anonymous@mail.ilc.edu.tw
146 anonymous@kh.edu.tw
147 anonymous@kl.edu.tw
148 anonymous@km.edu.tw
149 anonymous@matsu.edu.tw
150 anonymous@webmail.mlc.edu.tw
151 anonymous@ntct.edu.tw
152 anonymous@ntpc.edu.tw
153 anonymous@ptc.edu.tw
154 anonymous@tc.edu.tw
155 anonymous@tn.edu.tw
156 anonymous@tp.edu.tw
157 anonymous@dove.ttct.edu.tw
158 anonymous@stu.ttct.edu.tw
159 anonymous@tyc.edu.tw
160 anonymous@ylc.edu.tw
```


eduroam

- 那就來做個各校資料庫吧

 eduroam-eap-generic-CCU.eap-config	更新/新增設定檔、更新描述、新增手動建立教學等。
 eduroam-eap-generic-NCCU.eap-config	更新/新增設定檔、更新描述、新增手動建立教學等。
 eduroam-eap-generic-NCKU.eap-config	更新/新增設定檔、更新描述、新增手動建立教學等。
 eduroam-eap-generic-NCU.eap-config	更新/新增設定檔、更新描述、新增手動建立教學等。
 eduroam-eap-generic-NSYSU.eap-config	更新/新增設定檔、更新描述、新增手動建立教學等。
 eduroam-eap-generic-NTHU.eap-config	更新/新增設定檔、更新描述、新增手動建立教學等。
 eduroam-eap-generic-NTNU.eap-config	檔名錯誤修正
 eduroam-eap-generic-NTU.eap-config	更新/新增設定檔、更新描述、新增手動建立教學等。
 eduroam-eap-generic-NTUST.eap-config	更新/新增設定檔、更新描述、新增手動建立教學等。
 eduroam-eap-generic-NYCU.eap-config	更新/新增設定檔、更新描述、新增手動建立教學等。
 eduroam-eap-generic-TANetTestAdmin.eap-co...	更新/新增設定檔、更新描述、新增手動建立教學等。
 eduroam-eap-generic-TANetTestRc.eap-config	更新/新增設定檔、更新描述、新增手動建立教學等。
 eduroam-eap-generic-TWEdu-tested.eap-config	更新/新增設定檔、更新描述、新增手動建立教學等。



手搓？



不可能 絕對不可能

自動化

需要的資訊



使用者識別

使用者帳密



伺服器識別

伺服器憑證
伺服器網域



認證方式

PEAP-MSCHAPv2
TTLS-PAP
PEAP-GTC

需要的資訊



使用者識別

使用者帳密

使用者輸入



伺服器識別

伺服器憑證
伺服器網域



認證方式

PEAP-MSCHAPv2
TTLS-PAP
PEAP-GTC

RADIUS Server 測試 / 拿取

認證伺服器來源？



TANet 無線網路漫遊交換中心

Taiwan Academic Network Roaming



最新消息

漫遊介紹

相關文件

連線單位列表

各級高中職建置列表

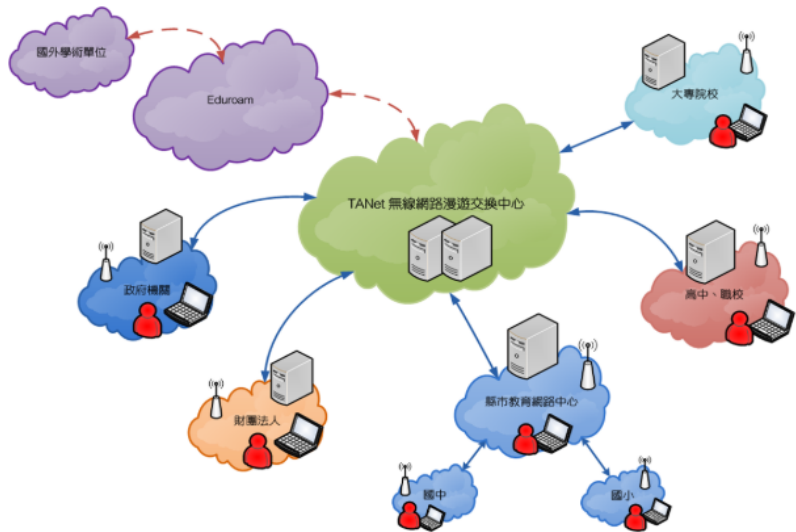
伺服器狀況

申請辦法

聯絡資訊

漫遊介紹

TANet無線網路漫遊交換中心將納入原本分別由國家高速網路中心以及資訊策進會介接之無線網路漫遊學術單位服務和國內非營利組織及國際學術相關無線網路，並與各個漫遊中心建立交換漫遊機制，讓所有使用TANet 網路單位的學生及都可以持單一帳號，以跨區憑證的方式享受與所屬單位相同的上網環境。(如下圖所示)





TANet 無線網路漫遊交換中心

Taiwan Academic Network Roaming



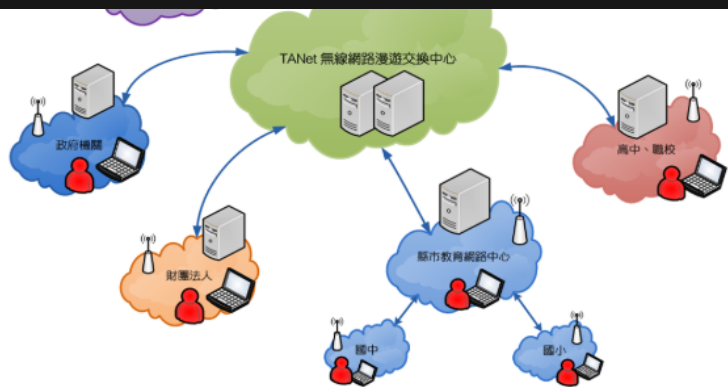
不，他們不會理我們的

歡迎漫遊中心打臉我

伺服器狀況

申請辦法

聯絡資訊



洩漏版？

- 南投資教
 - 他們之前洩漏了他們認證伺服器的連線資訊
 - 經測試有接跨校漫遊服務
 - 但我去年丟漏洞回報，他們修掉了
 - <https://zeroday.hitcon.org/vulnerability/ZD-2023-00885>

人才聚合 chilin

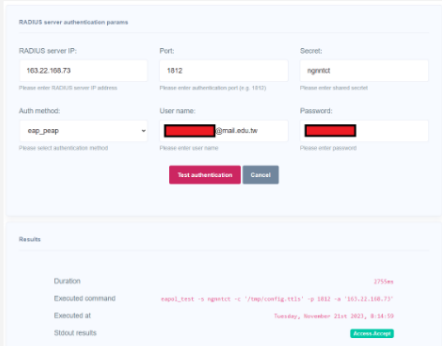
由該簡報第 13 頁可得知 Server IP 與 PreShare Key
嘗試 RADIUS 協定預設 Port 1812 可知其 Port
使用工具查詢網域，可知網域為 radiusdb.ntct.edu.tw
彙整以上資訊可得以下內容：

Server IP:
radiusdb.ntct.edu.tw
163.22.168.73

Port:
1812

PreShare Key:
ngnntct

由於是教育機構，因此懷疑有接入 TANet 無線網路漫遊交換中心，因此嘗試使用 eduoam 帳號送出驗證，得到驗證通過結果。
且取得正確的 CA 憑證。



The screenshot shows a web-based RADIUS server authentication tool. The 'RADIUS server IP' is set to 163.22.168.73, the 'Port' is 1812, and the 'Secret' is ngnntct. The 'Auth method' is set to eap_tls. The 'User name' is [redacted]@ntct.edu.tw and the 'Password' is [redacted]. A 'Test authentication' button is visible. Below the form, the 'Results' section shows a successful authentication with a duration of 270ms and a status of 'Success'.

拜託ATM
BATTLE

頂尖大學金頭腦爭霸戰
成功大學

TVBS 歡樂台 HD



我們是做好駭客



ChiLin.H 昨天 下午 01:14

抱歉打擾

想詢問一下我能不能把那張 "我們是做好駭客" 那張圖
放在我自己今年講 SITCON Lighting talk 的簡報裡



Vincent550102 昨天 下午 01:29

Go ahead XD



Vincent550102 Go ahead XD



ChiLin.H 昨天 下午 01:51

好耶 uwu

感謝 Vincent (已編輯)

我們是做好駭客

edu”roam”

全世界都能用，找其他國家有沒有能滿足需求的

認證資訊來源

- <https://eduroam.ustc.edu.cn/>
 - 國外開的帳號測試網頁
 - eapol_test
 - 從 log 裡面撈資料
- 僅 PEAP-MSCHAPv2 / TTLS-PAP 支援
- 做了一個假設：
 - 有憑證 == 可以認證
 - 但實際上可能非也

OpenSSL: RX ver=0x303 content_type=22 (handshake/certificate)

OpenSSL: Message - hexdump(len=3195): 0b 00 0c 77 00 0c 74 00 06 a4 30 82 06 a0 30 82 05 88 a0 03 02 01 02 02 10 47 e8 00 00 00 07 74 52 7c 05 8f 64 c8 e3 11 54 30 0d 06 09 2a 86 4a
TLS: tls_verify_cb - preverify_ok=1 err=20 (unable to get local issuer certificate) ca_cert_verify=0 depth=1 buf='/C=TW/O=TAIWAN-CA/CN=TWCA Secure SSL Certification Authority'
CTRL-EVENT-EAP-PEER-CERT depth=1 subject='/C=TW/O=TAIWAN-CA/CN=TWCA Secure SSL Certification Authority' hash=1a2c75fd096e0499e9ff6ac74e526f61eaae3edfc8c2ea4436fee0c24d8b7d0e
TLS: tls_verify_cb - preverify_ok=1 err=27 (certificate not trusted) ca_cert_verify=0 depth=1 buf='/C=TW/O=TAIWAN-CA/CN=TWCA Secure SSL Certification Authority'
CTRL-EVENT-EAP-PEER-CERT depth=1 subject='/C=TW/O=TAIWAN-CA/CN=TWCA Secure SSL Certification Authority' hash=1a2c75fd096e0499e9ff6ac74e526f61eaae3edfc8c2ea4436fee0c24d8b7d0e
TLS: tls_verify_cb - preverify_ok=1 err=27 (certificate not trusted) ca_cert_verify=0 depth=0 buf='/C=TW/ST=Taiwan/L=Taipei/O=Ministry of Education/CN=wifi.sso.edu.tw'
CTRL-EVENT-EAP-PEER-CERT depth=0 subject='/C=TW/ST=Taiwan/L=Taipei/O=Ministry of Education/CN=wifi.sso.edu.tw' hash=3ca16e8e8852673f300b45aed44cef0b2a6a0e0aed6790252140d047cea2484
CTRL-EVENT-EAP-PEER-ALT depth=0 DNS:wifi.sso.edu.tw <- 記錄他，等等填到 #Domain#

正將您輸入的信息发给radius服务器测试，测试结果汇总如下：

认证类型	测试结果
EAP-PEAP MSCHAPv2	FAILURE，认证失败
EAP-TTLS PAP	FAILURE，认证失败

结果说明：

FAILURE，认证失败：认证测试过程中出现了错误

OK，认证过程正常：认证环节正常

详细结果过程：

开始测试 EAP-PEAP MSCHAPv2 ...

使用的配置文件

```
network={
    ssid="eduroam"
    key_mgmt=wPA-EAP
    eap=PEAP
    identity="cart@mail.edu.tw"
    anonymous_identity="cart@mail.edu.tw"
    password="cart@mail.edu.tw"
    phase2="autheap=MSCHAPv2"
}
```

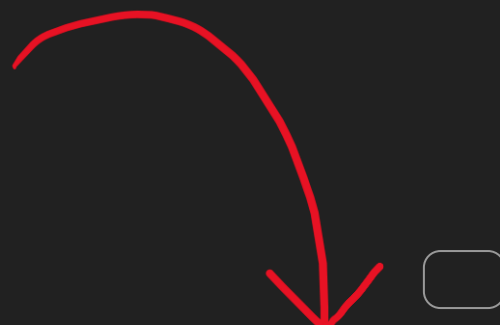
测试结果: FAILURE · 认证失败

```
Reading configuration file '/dev/shm/radcfg.6038.conf'
line: 1 - start of a new network block
ssid - hexdump_ascii(len=7):
    65 64 75 72 6f 61 6d                                eduroam
key_mgmt: 0x1
eap methods - hexdump(len=16): 00 00 00 00 19 00 00 00 00 00 00 00 00 00 00 00
identity - hexdump_ascii(len=16):
```

簡報、設定檔、其他資料請參閱 <https://edur.isli.me/>

設定檔

- 設定檔內容：**驗證方式 + 伺服器憑證**
- 適用範圍：
 - **PEAP-MSCHAPv2**
 - **TTLS-PAP**
 - PEAP-GTC 開發中 (等有機會可以直接連到漫遊中心)
- 下載連結 (資料陸續更新中)
 - <https://edur.isli.me/>
 - https://github.com/eduroamtw/geteduroam_tw
- 資訊錯誤 / 連不上回報
 - 連結：<https://edur.isli.me/>
 - 信箱：eduroamtw@googlegroups.com





那...
我可以連了吧



嗎？



國外

基本上都可以



台灣

要碰運氣

人為連線障礙 (x

EAP-Offload

- 部分服務提供者 (SP) 啟用
 - 運作過程和中間人攻擊手法 (MITM) 差不多
 - 會導致憑證和驗證方式被竄改
 - Lighting talk 沒時間完整解釋了
- TL;DR
 - 開了你就連不上網路



問題：憑證被串改

- 連線到 AP
- 裝置：憑證不一致，Reject
- User：連不上
 - 和右圖的狀況相同
- 設定不驗證伺服器憑證
 - ****非常危險****
 - 手機會直接傳帳密出去
 - 如果對方是惡意 AP，恭喜帳密外流
 - PEAP-GTC 甚至是直接傳明文帳密
 - GTC-Downgrade-Attack



你的連線不是私人連線

攻擊者可能會嘗試從 **wrong.host.badssl.com** 竊取你的資訊 (例如密碼、郵件或信用卡資訊)。 [進一步瞭解這項警告](#)

NET::ERR_CERT_COMMON_NAME_INVALID

[隱藏詳細資料](#)

[返回安全網頁](#)

伺服器無法證明其屬於 **wrong.host.badssl.com** 網域；其安全性憑證來自 *.badssl.com 網域。這可能是因為設定錯誤，或有攻擊者攔截你的連線所致。

[繼續前往 wrong.host.badssl.com 網站 \(不安全\)](#)

設定不驗證伺服器憑證

- Case:
- PEAP-GTC
- 不驗伺服器憑證
- 設定自動連線
- 使用者帳號連動校務系統 LDAP / Google 帳號，
且沒開 MFA
- 攻擊者在交通樞紐處放置假 AP
- **零操作盜帳號**

去年的 高雄資教 設定檔

<https://web.archive.org/web/20241203103200/https://wireless.kh.edu.tw/archives/121/>

高雄市政府教育局學校無線網路服務

無線網路服務摘要

校園無線網路連線 ▾

教學載具連線說明 ▾

Q&A

步驟2、手動設定SSID 802.1x 認證參數

KH

EAP 方法
PEAP

階段2 驗證
GTC

CA憑證
不進行驗證

您未指定任何憑證，因此無法為您設定個人連線。

識別
[Empty Field]

匿名識別
X 不須輸入

密碼
[Empty Field]

取消 連線

EAP方法：PEAP

階段2驗證：GTC

CA憑證：不進行驗證

識別：輸入帳號*

匿名識別：空白不輸入

密碼：輸入密碼*

點選連線


今年的 高雄資教 設定檔

然而他們 EAP-Offload 依舊沒關
所以高雄市資教帳號以外的帳號
不重寫設定檔依然連不上

高雄市政府教育局學校無線網路服務

[無線網路服務摘要](#)[校園無線網路連線](#)[教學載具連線說明](#)[Q&A](#)

步驟2、手動設定SSID 802.1x 認證參數



EAP方法：PEAP

階段2驗證：GTC

CA憑證：**使用系統憑證**

網域：**wireless.kh.edu.tw**

識別：輸入帳號*

匿名識別：空白不輸入，**如果有anonymous，請刪除**

密碼：輸入密碼*

點選連線

問題：EAP 方法被竄改

- 台灣主要三種 (加上內部二階認證的話)
 - PEAP-MSCHAPv2
 - TTLS-PAP
 - PEAP-GTC
- 上面這些可簡單理解成**語言**
- 語言不同，自然無法相互溝通
- 終端使用者幾乎無解決方案
- 我快講不完了所以只能講個概念，非常抱歉

解法 (緩解措施)

- 使用者：
 - **務必啟用伺服器憑證認證！**
 - 關閉 eduroam 自動連線，僅在學校手動連線
- 漫遊中心：
 - 強制統一規範 SP RADIUS 設定方式，禁止他們啟用會更改憑證的設定。
 - 強制統一規範 iDP 啟用憑證認證
- 校方：
 - **把 eduroam 帳密與其他校務系統獨立**
 - (部分學校) 換掉 Example Certificate Authority
 - Self sign 一個憑證，給使用者裝
 - Public CA

報告完畢

- 本次使用簡報、設定檔下載
 - edur.isli.me
 - 未來有新的也會同步更新
- chilin.h Blog
 - neko70.net
- e0pwr Personal Site
 - www.ichika.tw

