TANet無線網路漫遊交換中心

Taiwan Academic Network Roaming Center

校園無線網路EAP-802.1X建置暨eduroam認證

國立東華大學

聯絡方式

- 臺灣學術無線網路漫遊中心
  - https://roamingcenter.tanet.edu.tw/
- 服務電話
  - 03-9312047
- 聯絡信箱
  - pclee@ems.niu.edu.tw

摘要

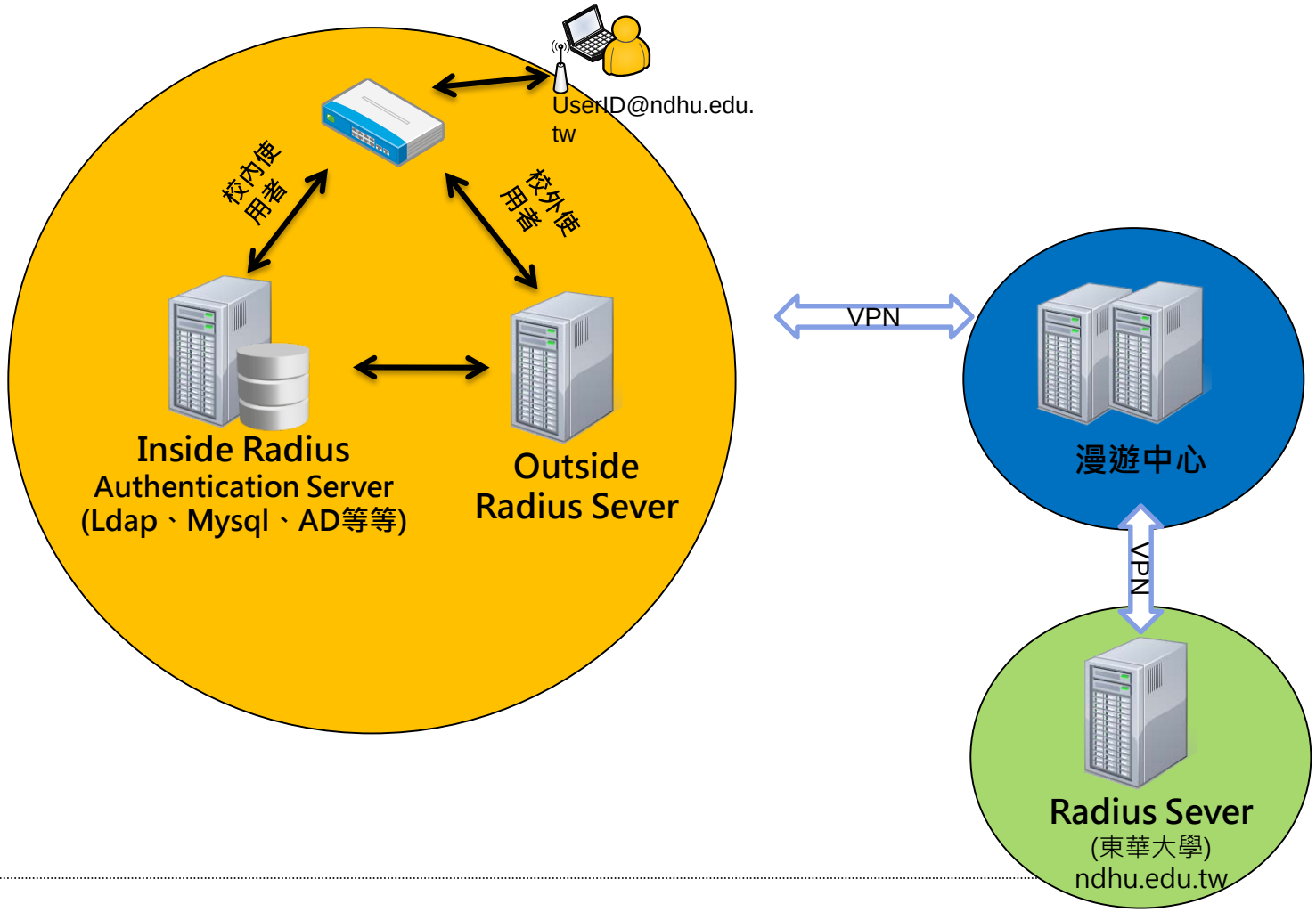
- eduroam簡介
- 加入eduroam流程
  - 無線控制器
  - Freeradius相關設定
- 加入eduraom常見問題

eduroam簡介

- eduroam 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。
- eduroam 的概念最初於2003被提出，並由歐洲位於五個不同國家的院校進行首次測試，繼而歐洲其他國家的教育機構和學術網絡相繼參與這個項目的建置，整個漫遊體系最 後被命名為 eduroam。

eduroam簡介

TANetRoaming架構圖



eduroam簡介

TANetRoaming和eduroam有什麼不同?

- 驗證機制
  - Web-based (TANetRoaming)
    - 現行大部分的連線登入驗證方式
    - 安全性較弱
    - 先取得IP後再以Web驗證方式上網
  - 802.1X (eduroam)
    - 安全性較強，傳輸資訊不易被竊取
    - 驗證完成後再取得IP上網
    - 只需認證一次，以後就不需再輸入帳密

加入eduroam流程

- eduroam簡介
- 加入eduroam流程
  - 無線控制器
  - Freeradius相關設定
- 加入eduraom常見問題

加入eduroam流程

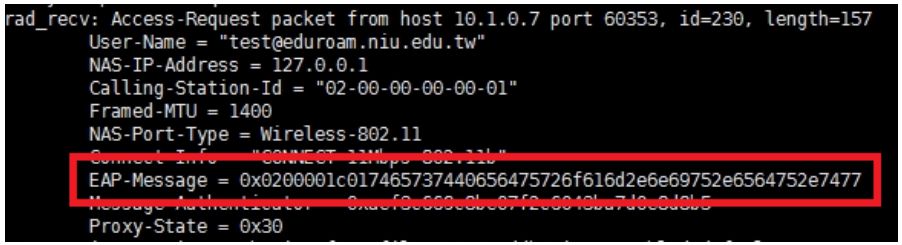
要如何部屬eduroam建置?

- **無線控制器**
  - 無線控制器設定需求
    - ✓SSID名稱必須為eduroam (小寫)
    - ✓須走擴展認證協議(EAP)
      - ➢ 常見有EAP-MSCHAPv2、EAP-GTC和EAP-TTLS
  - 漫遊中提供一組測試帳號請各單位測
    - ✓ID@eduroam.niu.edu.tw
  - 漫遊中心會觀察是否符合EAP-802.1X的驗證方式，完成單向測試
- **設定FreeRadius**
  - 請提供一組測試帳號給漫遊中心使用
  - 針對驗證伺服器做相關設定(eap.conf、inner-tunne和相關模組設定)
    - ➢Ldap
    - ➢Active Directory
    - ➢SQL

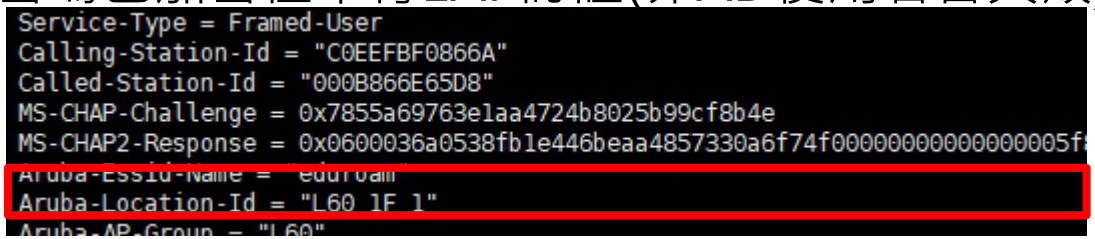
加入eduroam流程

無線控制器相關問題

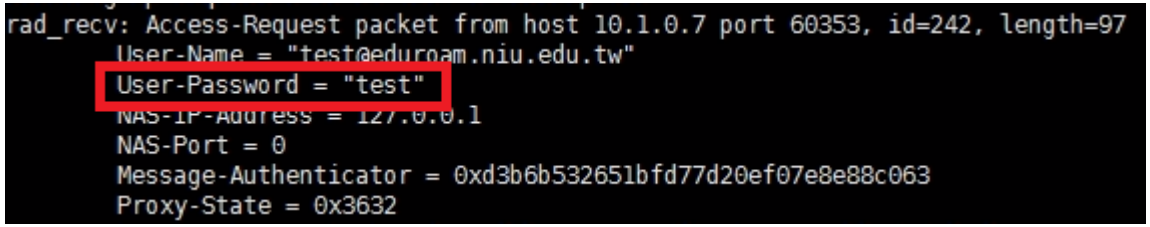
- 標準EAP認證方式



- 密碼已加密但不符EAP認證(非AD使用者會失敗)



- 未加密(國外使用者會失敗)



加入eduroam流程

無線控制器相關問題

- 標準EAP認證方式

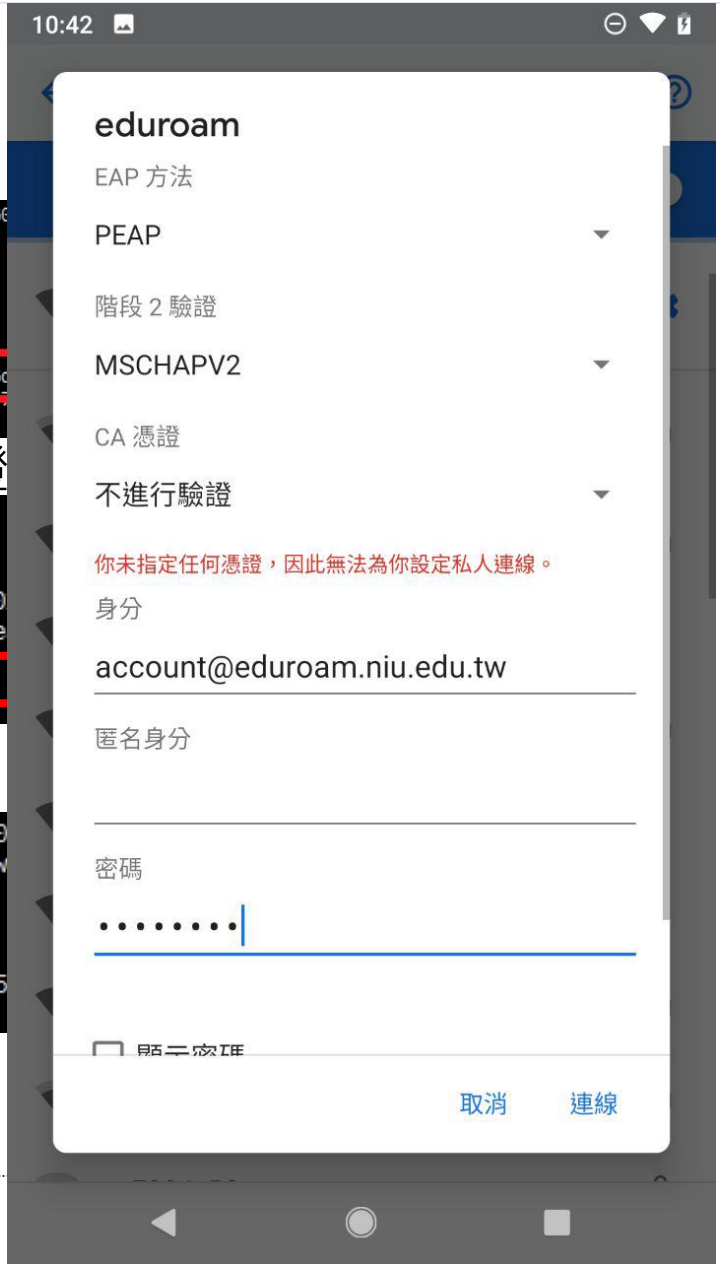
```
rad_recv: Access-Request packet from host 10.1.0.7 port 6
        User-Name = "test@eduroam.niu.edu.tw"
        NAS-IP-Address = 127.0.0.1
        Calling-Station-Id = "02-00-00-00-00-01"
        Framed-MTU = 1400
        NAS-Port-Type = Wireless-802.11
        EAP-Message = 0x0200001c0174657374406564756f616c
        Proxy-State = 0x30
```

- 密碼已加密但不符EAP認證

```
Service-Type = Framed-User
Calling-Station-Id = "C0EEFBF0866A"
Called-Station-Id = "000B866E65D8"
MS-CHAP-Challenge = 0x7855a69763e1aa4724b80
MS-CHAP2-Response = 0x0600036a0538fb1e446be
Aruba-Essid-Name = "eduroam"
Aruba-Location-Id = "L60 1F 1"
Aruba-AP-Group = "L60"
```

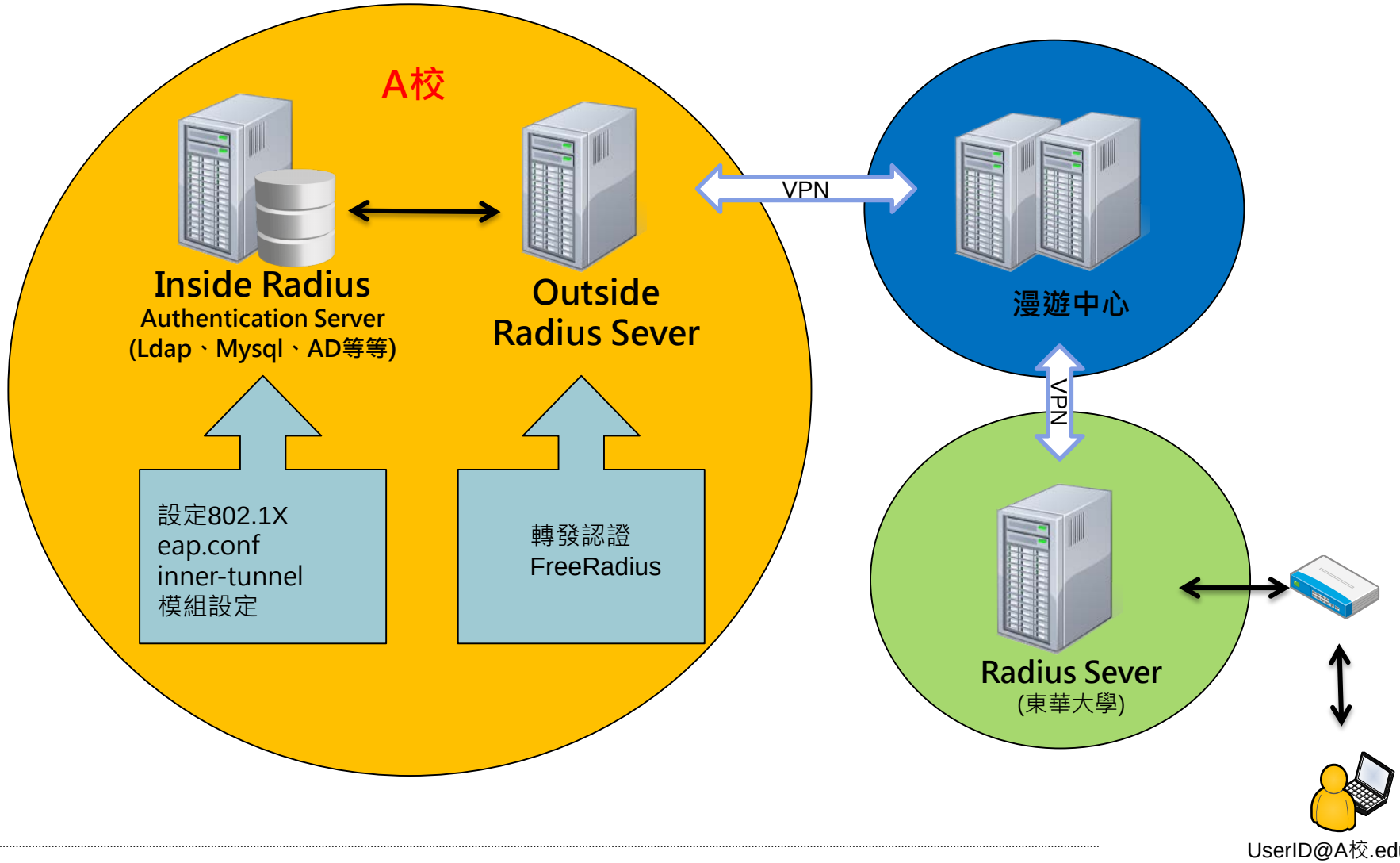
- 未加密(國外使用者會失敗)

```
rad_recv: Access-Request packet from host 10
        User-Name = "test@eduroam.niu.edu.tw"
        User-Password = "test"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 0
        Message-Authenticator = 0xd3b6b53265
        Proxy-State = 0x3632
```



加入eduroam流程

設定FreeRadius

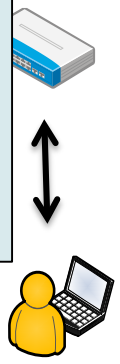


加入eduroam流程

設定FreeRadius

主要設定檔

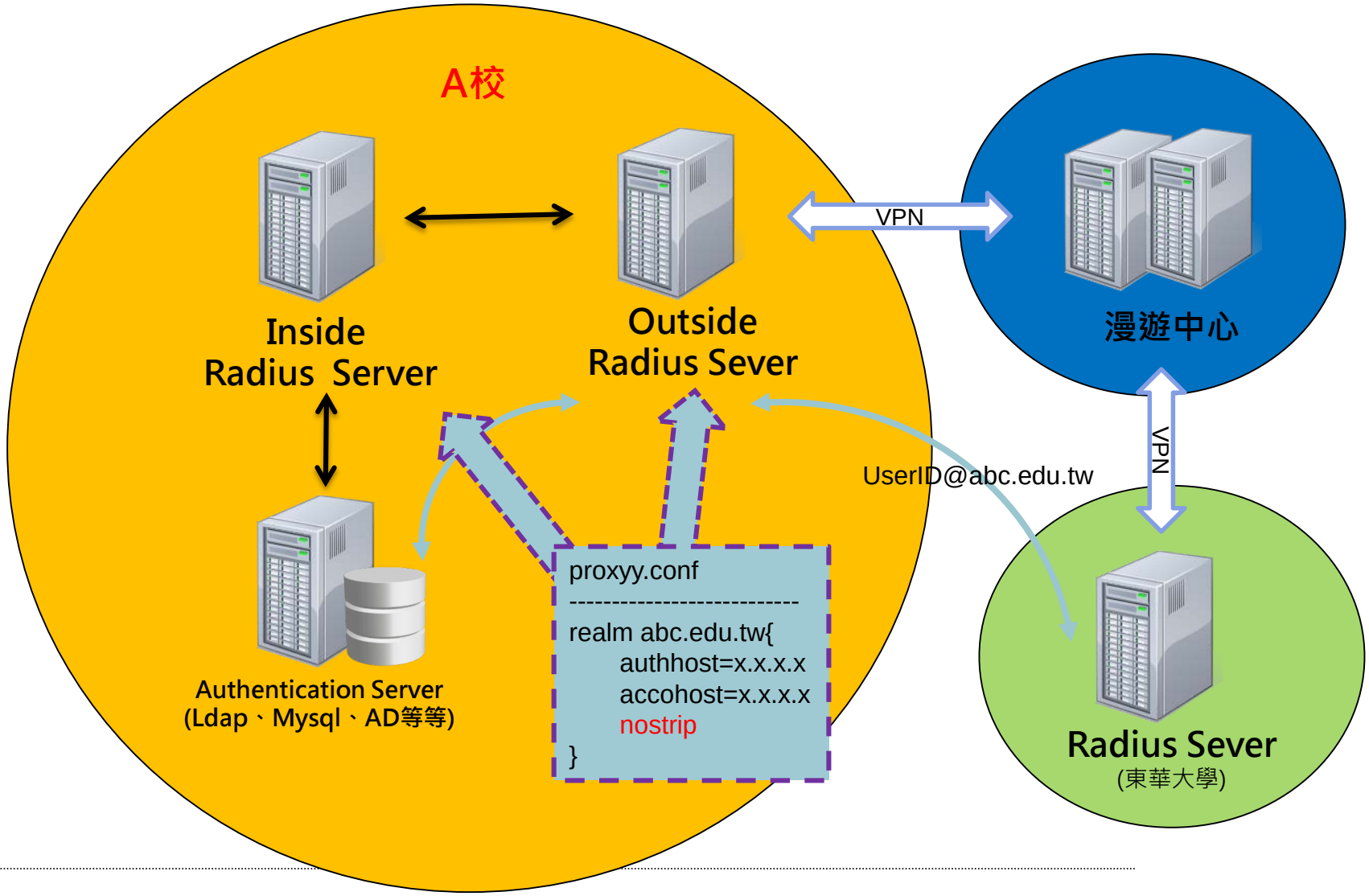
- /etc/raddb/
  - eap.conf (初始EAP解密方法)
  - proxy.conf (轉發認證)
- /etc/raddb/sites-available/
  - default (預設設定方式)
  - inner-tunnel (EAP設定方式)
- /etc/raddb/modules/
  - ldap(認證模組)
  - sql(認證模組)
  - Mschapv2(認證模組)
- /etc/raddb/certs(部屬憑證)



UserID@A校.edu.tw

加入eduroam流程

設定FreeRadius(轉發認證)



加入eduroam流程

設定加密機制方式

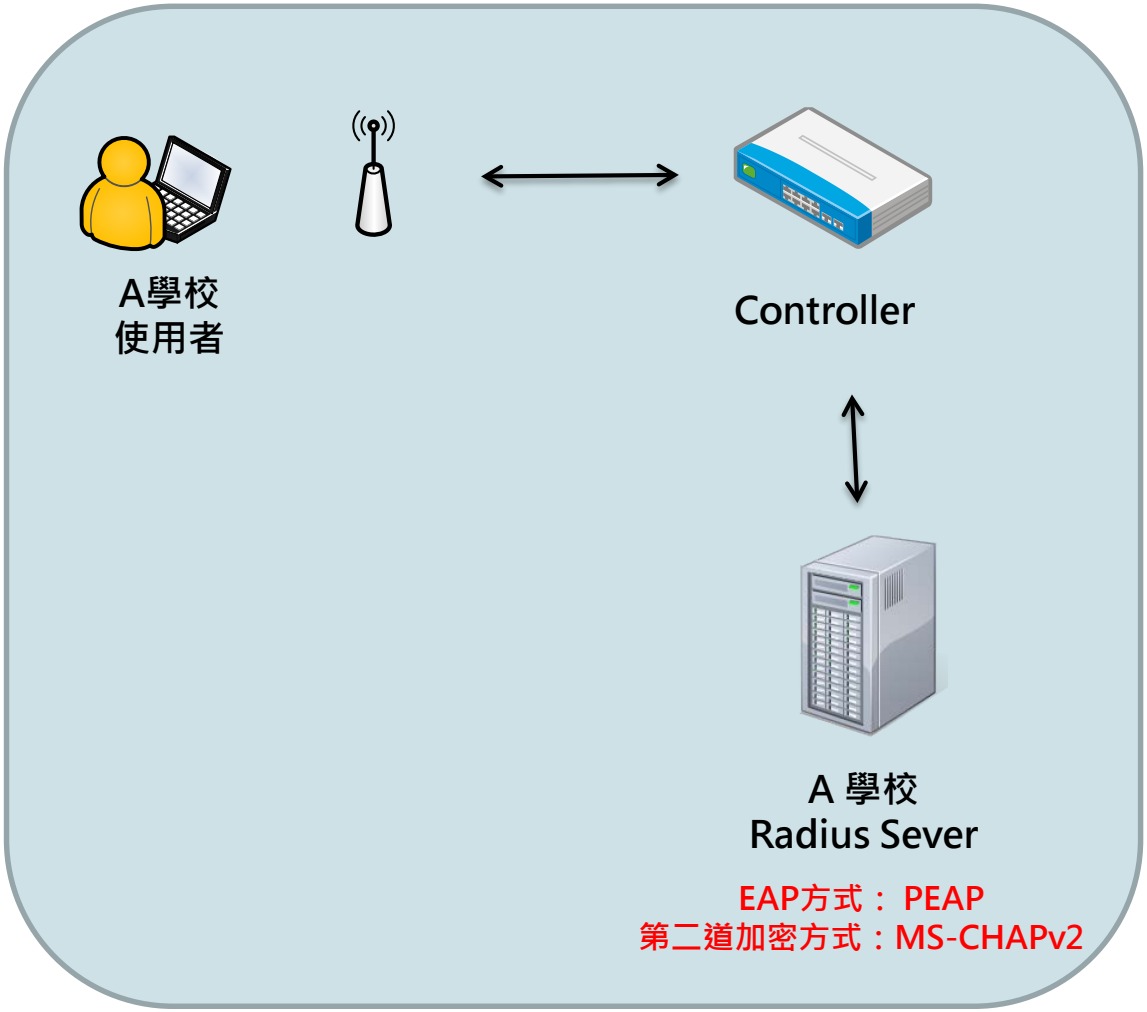
	Clear-text	NT hash (ntlm_auth)	MD5 hash	Salted MD5 hash	SHA1 hash	Salted SHA1 hash	Unix Crypt
PAP	✓	✓	✓	✓	✓	✓	✓
CHAP	✓	x	x	x	x	x	x
Digest	✓	x	x	x	x	x	x
MS-CHAP	✓	✓	x	x	x	x	x
PEAP	✓	✓	x	x	x	x	x
EAP-MSCHAPv2	✓	✓	x	x	x	x	x
Cisco LEAP	✓	✓	x	x	x	x	x
EAP-GTC	✓	✓	✓	✓	✓	✓	✓
EAP-MD5	✓	x	x	x	x	x	x
EAP-SIM	✓	x	x	x	x	x	x
EAP-TLS	x	x	x	x	x	x	x

摘要

- eduroam簡介
- 加入eduroam流程
  - 無線控制器
  - Freeradius相關設定
- 加入eduraom相關問題

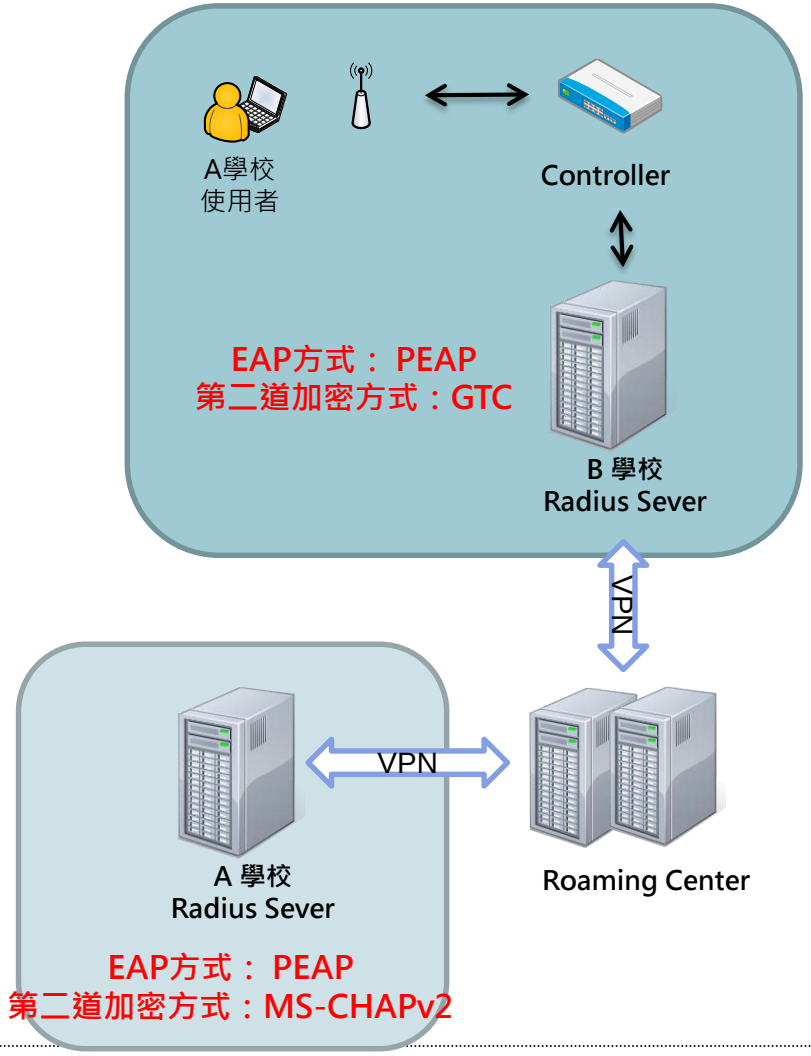
加入eduroam相關問題

EAP-802.1X驗證問題-使用者連線問題



加入eduroam相關問題

EAP-802.1X驗證問題-使用者連線問題



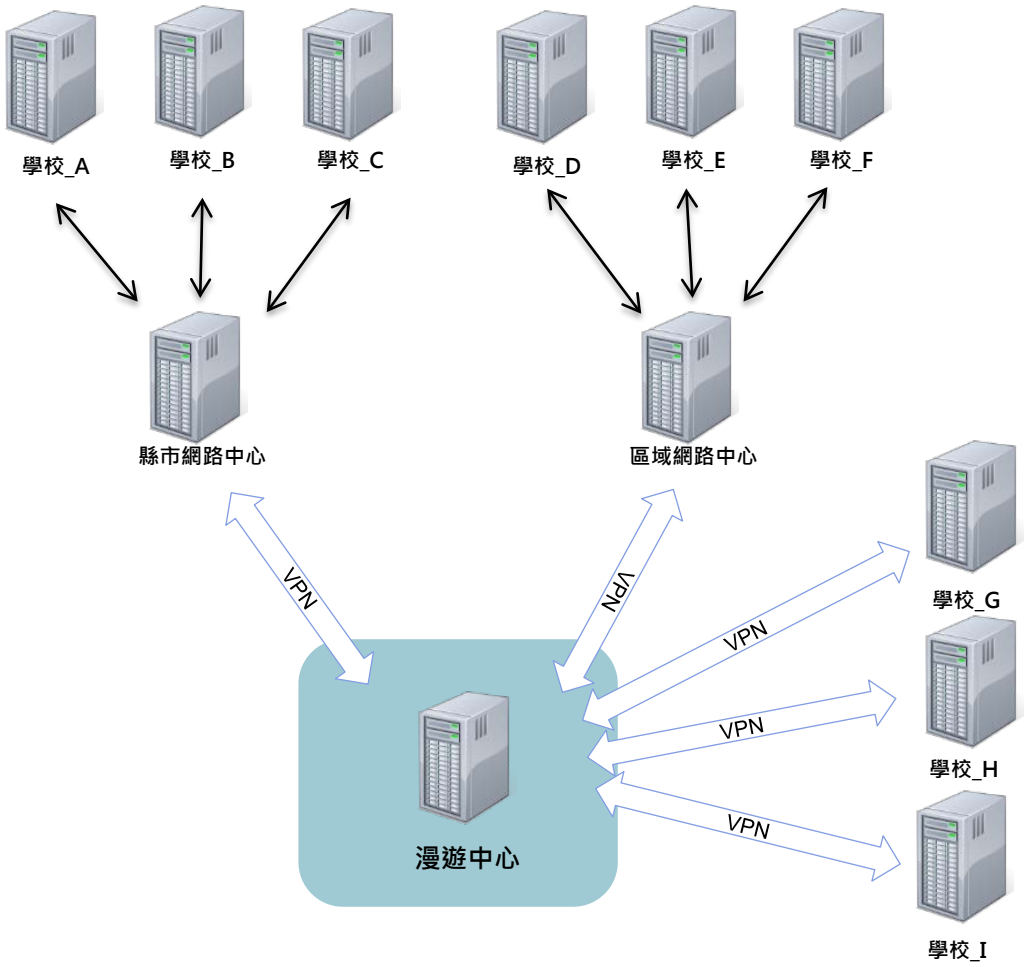
加入eduroam相關問題

EAP-802.1X常見問題

- 建置問題
  - ✓ SSID名稱必須為eduroam (小寫)
  - ✓ 須走擴展認證協議(EAP)
    - 常見有PEAP-MSCHAPv2、PEAP-GTC和EAP-TTLS
  - ~~✓ 無線控制器須提供：Accounting Log(AAA服務)~~
- 教育問題
  - ✓ 使用者教育問題
    - **強烈建議**，當使用者登入eduroam服務或是TANetRoaming時，不管校內、校外**必須**打全部名稱(例：UserID@ndhu.edu.tw)
    - 建議辦理教育訓練、或是建置手冊減少網管人員負擔
- 頻寬問題

加入eduroam相關問題

前瞻機計畫相關問題



加入eduroam相關問題

802.1X測試工具(wpa_supplicant)

- 創立一個測試檔案(test.conf)

```
network={
    ssid="eduroam"
    key_mgmt=WPA-EAP
    eap=TTLS        #第一階段驗證方式
    identity="test@test.niu.edu.tw"        #要驗證的使用者帳號
    password="test"         #要驗證的使用者密碼
    phase2="auth=PAP"       #第二階段加密方式
}
```

- 測試方式

```
#eapol_test   -c   test.conf   -a   127.0.0.1   -s   testing123
```

- 測試結果

  SUCCCESS or FAILURE

加入eduroam相關問題

		認證交換					認證交換		
連線單位	前瞻計畫	漫遊中心	縣市網路中心	區域網路中心	連線單位	前瞻計畫	漫遊中心	縣市網路中心	區域網路中心
長榮高級中學		✓			鳳和高級中學				
長榮女子高級中學		✓			臺南市立大灣高級中學	✓	✓		
國立臺南第二高級中學		✓			臺南市立南寧高級中學	✓			
國立臺南女子高級中學	✓	✓			臺南市立土城高級中學	✓			
國立臺南第一高級中學	✓	✓			臺南市立永仁高級中學	✓			
國立臺南大學附屬高級中學	✓	✓			國立南科國際實驗高級中學	✓			
國立北門高級中學	✓	✓			慈濟高級中學				
南光高級中學					臺南市私立南英高級商工職業學校				
國立新營高級中學	✓	✓			國立臺南高級工業職業學校	✓	✓		
國立臺南家齊高級中等學校	✓	✓			國立臺南高級商業職業學校	✓	✓		
光華高級中學		✓			國立臺南高級海事水產職業學校	✓			
國立後壁高級中學	✓	✓			國立曾文高級農工職業學校	✓			
國立新豐高級中學	✓	✓			國立新化高級工業職業學校	✓	✓		
國立善化高級中學	✓				國立白河高級商工職業學校	✓	✓		
六信高級中學					國立曾文高級家事商業職業學校	✓	✓		
國立新化高級中學		✓			國立新營高級工業職業學校	✓	✓		
瀛海高級中學					國立北門高級農工職業學校	✓	✓		
崑山高級中學		✓			臺南市私立慈幼高級工商職業學校		✓		
天主教德光高級中學					臺南市私立陽明高級工商職業學校				
天主教黎明高級中學		✓			臺南市私立育德工業家事職業學校				
天主教聖功女子高級中學					臺南市私立亞洲高級餐旅職業學校				
港明高級中學		✓			國立玉井高級工商職業學校	✓	✓		
興國高級中學		✓			國立成功大學附設高級工業職業進修學校				
明達高級中學					國立臺南啟智學校	✓	✓		
新榮高級中學					國立臺南大學附屬啟聰學校	✓			
					統計	26	28	0	0

加入eduroam相關問題

目前完成雙向驗證學校

eduroam members

National Taiwan Normal University

National Chiao Tung University

National Tsing Hua University

National Hsinchu University of Education

National Taipei University

Tatung University

National Ilan University

Shih Chien University

National Dong Hwa University

Fortune Institute of Technology

Taiwan Academic Network Educational Net Center of Chia Yi County

Ministry of Education

加入eduroam相關問題

申請eduraom臨時帳號

eduroam 帳號申請表			
機密等級	敏感	版次	1.0

紀錄編號：_____　　填表日期：　年　月　日

申請人資料（請確實填寫，不可空白，否則不予受理）：

中文姓名：_____

帳號名稱 1：_____(範例：Kevin_chen)

帳號名稱 2：_____(範例：Kevin_chen201710)

服務單位、職稱（學生請填科系、班級）：_____

注意事項：

✧ **已申請者不得重複申請。**
✧ **帳號、密碼請熟記，並妥善保管，不受理任何查詢帳號、密碼之申請。**

申請人應遵守下列使用規定：

✧ 帳號僅限本人使用，不得借予他人。如經查覺有借用情形，則立即停止該帳號的使用權，往後亦不得再申請。
✧ 申請者須遵守台灣學術網路使用規範。
✧ 其他未盡事宜，悉依現行法令規定辦理。

申請單位簽章：_____（保證所填資料正確無誤，並願遵守使用規定）

漫遊中心審核（申請人請勿填寫）：

准予使用：

帳號：_____@admin.edu.tw　　密碼：_____

使用期限：_____

備註：

END